Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope.**

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery**. Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty**.

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination**.

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract

Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users.** Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source.** Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the “Support Schedule”), the Entrust General Terms and Conditions (“General Terms”)**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. “**Business Day**” means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. “**Covered Offering**” means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. “**Customer-Hosted Offering**” means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer’s premises.

1.4. “**Extended Support**” means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. “**Hosted Service**” for the purposes of this Schedule means Entrust’s Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. “**Incident**” means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. “**Named Support Contacts**” means individual Users nominated by Customer to act as Customer’s support representatives.

1.8. "**Problem**” means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. “**Production Environment**” means Customer’s live business environment with active users.

1.10. “**Response Time**” means the amount of time that elapses between the Customer’s report of a Service Request to Entrust and Entrust’s acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. “**Service Plan**” means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**” means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. “**Software**” for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. “**Superseded Product**” means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. “**Support Services**” means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. “**Upgrade**” in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees.**

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer’s Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. “Second Line Support” means (i) communicating with Customer’s Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust’s control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail (“Immediate Incident Response Time”).

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust’s sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust’s Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer’s business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. **Upgrades for Customer-Hosted Offerings**.

   8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

   8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions**.

   9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).
   9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.
   9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of

the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause.

Certificate and Signing Services
Terms of Use

The Agreement for Entrust's Certificate Services, any digital Signing Services, Time-stamping Services and/or Dedicated CAs is made up of these terms of use (the "ECSS Schedule"), the CPS and/or TPS (each defined below), the Entrust General Terms and Conditions ("General Terms") and an Order for Certificate Services, Signing Services, and/or Dedicated CAs. Capitalized terms not defined herein have the meanings given to them in the General Terms.

For clarity, the parties acknowledge and agree that the Agreement as defined above constitutes the subscriber agreement, as required and defined in the Industry Standards, for all Certificates issued hereunder.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE HOSTED SERVICES. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICES IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. <u>Definitions</u>.

1.1. "**Application Software Vendor**" or "**ASV**" means a developer of Internet browser software, email software or other software that displays or uses Certificates, including but not limited to Adobe, Apple, Google, Intel, Microsoft, Mozilla, and Oracle.

1.2. "**Certificate**" means a digital document that at a minimum: (a) identifies the certification authority issuing it, (b) names or otherwise identifies a Subject; (c) contains a public key of a key pair, (d) identifies its operational period, (e) contains a serial number and (f) is digitally signed by the certification authority. There are various types of Certificate(s) that may be issued to Subscriber by Entrust depending upon the Certificate Services that have been purchased, for example (and not exhaustively) OV SSL Certificates, extended validation ("**EV**") SSL Certificates, OV code signing Certificates, EV code signing Certificates, document signing Certificates, verified mark Certificates ("**VMC**s"), mobile device Certificates, private SSL Certificates, SMIME Certificates, eIDAS qualified website authentication Certificates ("**eIDAS QWAC**s"), PSD2 qualified website authentication Certificates ("**PSD2 QWAC**s"), eIDAS qualified seal certificate(s) ("**eIDAS QSealCs**"), PSD2 qualified Seal Certificate(s) ("**PSD2 QSealCs**"), and eIDAS Qualified Signature Certificate(s) ("**eIDAS QSigCs**").

1.3. "**Certificate Beneficiaries**" means, collectively, all Application Software Vendors with whom Entrust has entered into a contract to include Entrust's root Certificate(s) in such ASV's software, and all Relying Parties that actually rely on such Certificate during the period when it is Valid.

1.4. "**Certificate Services**" means the services offered by Entrust relating to the issuance, management and revocation of one or more Certificate(s), including Foreign Certificate Management Right(s), and includes any Certificate(s) issued to or for Customer pursuant to the Agreement.

1.5. "**CPS**" means the most recent version of the certification practice statement that is incorporated by reference into the Certificate(s) that are issued by Entrust, as may be amended from time to time in accordance with the terms of the CPS, and which is also hereby incorporated by reference into the Agreement. The CPS applicable to a specific Certificate depends on the type of Certificate and can be found on the Internet at http://www.entrust.net/cps or by contacting Entrust. For example, eIDAS QWACs and PSD2 QWACs are governed by the most recent version of the document titled "Certification Practice Statement For Qualified Certificates", private SSL Certificate(s) are governed by the most recent version of the document titled "Certification Practice Statement For Private Trust Certificates", and other Certificates are generally governed by the most recent version of the document titled "Certification Practice Statement".

1.6. "**Dedicated CA**" means an issuing certification authority chaining up to one of Entrust's public root CAs dedicated to issuing Certificates for Customer.

1.7. "**Foreign Certificate(s)**" means any Certificate that was not issued to or for Customer under this ECSS Schedule. For greater certainty, Foreign Certificates may include, but are not limited to, Certificates issued from other management services accounts, Certificates purchased from Entrust's retail web site, Certificates issued from other Entrust service offerings (for example, PKI as a Service), and Certificates issued by any third party.

1.8. "**Foreign Certificate Management Right(s)**" means an optional license enabling Customer to use its Management Account to receive certain management services (as set out in the Documentation) for one (1) Foreign Certificate for each Foreign Certificate Management Right(s) purchased by Customer. The quantity of Foreign Certificate Management Right(s) available to Customer will be tracked by its Management Account and Customer's inventory of available Foreign Certificate Management Right(s) will be increased or decreased by a quantity corresponding to the number of Foreign Certificates added to or released from its Management Account.

1.9. "**Hosted Services**" means, in this ECSS Schedule, the specific Certificate Services and any Time-stamping Services, Signing Services and/or Dedicated CAs that Customer has purchased as specified in the Order, and includes a Management Account.

1.10. "**Industry Standards**" means, collectively, the most up-to-date versions of each of the following, in each case, that are applicable to the various types of publicly-trusted Certificates and Time-stamps issued by Entrust, and to which Entrust is subject and bound as an issuer of such Certificates and Time-stamps:

1.10.1. the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

1.10.2. the CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Certificates ("EV Guidelines"),

1.10.3. the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Code Signing BRs"),

1.10.4. European Standards produced by the ETSI Technical Committee Electronic Signatures and Infrastructures,

1.10.5. the Minimum Security Requirements for Issuance of Verified Mark Certificates approved by the Authindicators Working Group for VMCs ("VMC Requirements"), and

1.10.6. laws and regulations.

1.11. "**Management Account**" means a self-service administration tool hosted by Entrust that identifies Customer by its full legal name in the "Customer Name" field, tracks Customer's entitlements with respect to the Hosted Services and enables Customer, as applicable in accordance with its entitlements, to manage the issuance, revocation, and expiry of one or more Certificate(s) and access and use the Signing Services.

1.12. "**Relying Party**" means any individual or entity that relies on a Valid Certificate or on a Time-Stamp. For avoidance of doubt, an ASV is not a "Relying Party" when software distributed by such ASV merely displays information regarding a Certificate.

1.13. **"Signing Services"** means the services offered by Entrust relating to the generation, management and hosting of keys to sign hashed data.

1.14. "**Subject**" means the Person or device identified in the "Subject" field in a Certificate.

1.15. "**Subscriber**" means the Person who applies for or is issued a Certificate.

1.16. "**Suspect Code**" means any code or set of instructions that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the computing environment on which it executes.

1.17. "**Time-stamp**" means data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

1.18. “**Time-stamping Services**” means the services offered by Entrust relating to the issuance of one or more Time-stamp(s), and includes any Time-stamp(s) issued to or for Customer pursuant to the Agreement.

1.19. “**TPS**” means the most recent version of the timestamping practice statement describing the practices followed by Entrust in issuing Time-stamp(s), as may be amended from time to time in accordance with the terms of the TPS, and which is also hereby incorporated by reference into the Agreement. The TPS applicable to a specific Time-stamp depends on the type of Time-stamp and can be found on the Internet at http://www.entrust.net/cps or by contacting Entrust.

1.20. “**Users**” has the meaning set out in the General Terms, and in this ECSS Schedule, includes Customer’s Agents and all Persons who are Subjects and Subscribers of Certificates and Time-stamps issued using Customer’s Management Account.

1.21. “**Valid**” means that a Certificate has not expired and has not been revoked.

2. Operation of the PKI. Each CPS and TPS sets out Entrust’s practices for managing the public-key infrastructure for the Hosted Services and providing the types of Certificates identified in the CPS and Time-stamps identified in the TPS, including:

(a) Specification of the applicable Industry Standards and policies;
(b) Information for Relying Parties;
(c) Event log retention period;
(d) Procedures for complaints and dispute settlement;
(e) Specification of the applicable compliance audits and other assessments;
(f) Contact information for questions about Certificates and Time-stamps;
(g) How revocation status information is provided and the period over which it is available.

3. Hosted Services Details. Provision of Hosted Services. Entrust will generate, provide and operate the Hosted Services in accordance with the applicable CPS, TPS, Documentation, and Customer’s Order(s) for the Hosted Services. Without limiting the foregoing:

3.1. Certificate Services—Verification, Issuance and Revocation of Certificate(s). Upon receipt of an application for a Certificate, Entrust will perform the limited verification of the information contained in the application as described in the CPS for the applicable type of Certificate. After completing such verification, Entrust will issue Certificate(s) and make them available for retrieval and management if and as set out in the CPS, the Documentation, and Customer’s entitlements under its Order for Certificate Services. Entrust may reject applications for Certificates for the reasons set out in the CPS. Entrust is entitled to revoke a Certificate it has issued if revocation is requested by Customer, upon expiry or termination of the Agreement, or for any other reason identified for revocation in the Agreement, the CPS or the Industry Standards.

3.2. Signing Services. Upon receipt of a request for key generation, Entrust will generate and host a key pair, and make the keys available for Customer’s use in connection with a Certificate for which Customer or one of its Affiliates is the Subscriber and/or the Subject, all if and as set out in the CPS, the Documentation, and Customer’s entitlements under its Order for Signing Services.

3.3. Time-stamping Services. Upon receipt of a request for a Time-stamp, Entrust will issue a Time-stamp, all if and as set out in the TPS, the Documentation, and Customer’s entitlements under its Order for Time-stamping Services.

3.4. Dedicated CA. If an Order calls for one or more Dedicated CA(s) to be provided for Customer’s use, Entrust will host and operate each Dedicated CA in accordance with the CPS, Documentation, and Customer’s entitlements under its Order for the Dedicated CA. The details of the Dedicated CA, such as the Subject to be identified in the Dedicated CA Certificate, the types of Certificate that will be issued by the Dedicated CA, and any other limitations or requirements, will be specified in a written addendum mutually executed by the parties, or in the Order for the Dedicated CA. Any Dedicated CA addendum is hereby included in the “Agreement” for the Dedicated CA. The Dedicated CA and its keys will be owned and controlled by Entrust. The validity period of the CA Certificate for a Dedicated CA will be no longer than that of the root CA that issued it, but may be revoked by Entrust if revocation is requested by Customer, upon expiry or termination of the Offering Term, or for any other reason identified for revocation in the Agreement, the CPS or the Industry Standards.

3.5. Hosted Service Revisions. Entrust may modify Hosted Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to a Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice on Entrust's website constitutes written notice). In the event that an Entrust change has a material detrimental impact on the Hosted Service that Customer has purchased, Customer may elect to terminate the affected Hosted Service and Customer shall be entitled to a pro rata refund for any fees pre-paid by Customer for the portion of the affected Hosted Service not yet provided or delivered by Entrust as of the date of termination.

4. Grant of Rights.

4.1. General Use. Subject to Customer (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Services, and to grant its Users the ability to access and use the Hosted Services, and to distribute Certificates issued by the Certificate Services, in each case solely (a) in accordance with this ECSS Schedule and the CPS and/or TPS, as applicable; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Hosted Services that Customer is permitted to use, such as limits associated with subscription types or levels, and on numbers or types of Certificates, Time-stamps, identities, Users, signatures or devices purchased; and (d) subject to the general restrictions set out in Section 3 of the General Terms (Restrictions).

4.2. Evaluation Use. At Entrust's discretion, it may provide Customer with access to and right to use any of the Hosted Services for evaluation purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Section 4.2 (Evaluation Use) or a separate evaluation agreement executed by the parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms, this ECSS Schedule, the CPS and/or TPS, as applicable, and an applicable Order (if any), for sixty (60) days Customer may, solely as necessary for Customer's evaluation of a Hosted Service, access and use the Hosted Service exclusively in, from and/or in connection with a Customer test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data). For clarity, Certificates issued in connection with an evaluation of Certificate Services ("Trial Certificates") shall have a maximum operational period of 60 days and may not be used for production purposes. Performance and security testing is expressly excluded from evaluation purposes and is strictly prohibited. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 4.1 (General Use), 8 (Support Services), 14.1 (Offering Term) and 19 (Publicity) do not apply to any evaluation of the Hosted Service. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Service at any time, for any or no reason, without advance notice. Customer will revoke any and all outstanding Trial Certificates when Customer has completed the evaluation but in all cases prior to the termination of the evaluation period or any trial account created for the evaluation. Customer hereby authorizes Entrust to revoke any and all outstanding Trial Certificates upon the termination of the evaluation period or any trial account created for the evaluation.

5. Customer Roles, Responsibilities, and Representations and Warranties.

5.1. Agents. A Subscriber may exercise its rights and obligations with respect to the Certificate Services through Customer or through certain Users appointed to fulfill the roles set out in Exhibit A, subject to any applicable verification or confirmation requirements set out in the CPS, such as verification that a person requesting EV Certificates is a verified 'Certificate Requester' under the EV Guidelines ("Agents"). The appointed Agents may be identified in Exhibit A, or will be provided to Entrust during enrollment. Such appointment may be modified using means established by Entrust from time to time. Subscriber agrees that Entrust is entitled to rely on instructions provided by the Agents with respect to the Hosted Services as if such instructions were provided by the Subscriber itself.

5.2. Signing Service Users. Customer may exercise its rights and obligations with respect to the Signing Services through certain Users appointed by Customer in its discretion ("**Signing Service Users**"). Such appointment may be modified using means established by Entrust from time to time. Customer agrees that it is responsible for Signing Service Users' compliance with the Agreement and for the Signing Service Users' use of the keys hosted by the Signing Services.

5.3. Representations and Warranties. Customer will comply with the requirements set forth in Exhibit B as applicable to Customer when it acts in the capacity of Subscriber or Subject. Customer will notify all Customer Affiliates, Users and any other Persons who act in the capacity of Subscriber, Subject, Agent or Signing Service User (e.g. apply for, receive, are issued, or manage Certificates, or use Signing Services to generate keys and/or sign hashed data) under this ECSS Schedule through Customer's Management Account that they are required to comply with the requirements set forth in this Agreement (including those set out in Exhibit B) as applicable to the activities and roles of Subscribers, Subjects, Agents and Signing Service Users in connection with the Hosted Services and Certificates, and Customer will be responsible for ensuring such compliance. Customer represents and warrants to Entrust and all Certificate Beneficiaries that Customer has the authority to bind all Subscribers to the Agreement if and to the extent that such Subscribers are issued any Certificate(s) under this ECSS Schedule through Customer's Management Account. Customer represents and warrants that each of its Signing Service Users has or will have obtained any requisite rights and authorizations for Signing Service Users' use of the keys hosted by the Signing Services.

5.4. Separate Subjects. For certain Certificates, as permitted by the applicable CPS, e.g. mobile device Certificates, SMIME Certificates, and certain document signing Certificates ("Client Certificates"), the Subject of the Certificate may be an individual who is different from the Subscriber. If Customer's Order entitles it to any Client Certificates, Customer agrees that such Client Certificates will only be issued and distributed to such Subjects pursuant to the most recent version of the Client Certificate Agreement that can be found at http://www.entrust.net/cps and provided that (i) Subscriber has verified the information included in each Client Certificate as being accurate; (ii) the individual to whom such Client Certificate is issued has consented to the inclusion of all data that is incorporated into such Client Certificates; (iii) the individual to whom such Client Certificate is issued has been notified of its obligations pursuant to Section 5.3 (Representations and Warranties) above and (iv) such Client Certificate is used only for Subscriber-related business.

5.5. Customer-hosted Components. If Customer's Order for a Hosted Service includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Service (collectively, "Customer-hosted Products"), Customer will be responsible for the lifecycle management (patching, upgrades, etc.) of such Customer-hosted Products and the security of the environment where it installs and uses such Customer-hosted Products. Customer will implement commercially reasonable security measures with respect to the Customer-hosted Products and the environment where they are installed. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures; and (ii) for any Customer-hosted Products that are or include software, always use the current version of such software and promptly install any security patches and any upgrades/updates required for proper functioning of all features of the Hosted Service. Customer understands if it fails to comply with this Section it could create a security risk and/or otherwise negatively impact the operation of the Hosted Service and Entrust may have the right to suspend the Hosted Service in accordance with Section 15 (Suspension). In addition, Customer may not be able to access new features or functions of the Hosted Service if it does not comply with this Section.

5.6. Network Requirements. Customer is responsible for procuring, maintaining, monitoring and supporting its communications infrastructure, network (LAN or WAN), and all components that connect to the Hosted Service(s). Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure, nor for any service degradation or failures caused by network connectivity of such external infrastructure.

5.7. Devices. For Certificates issued to devices, Customer is responsible for ensuring that the relevant devices support and are interoperable with the Certificates.

5.8. Unauthorized Access. Customer will take all reasonable steps to prevent unauthorized access to the Hosted Services, including by securing, protecting and maintaining the confidentiality of its access credentials. Customer is responsible for any access and use of the Hosted Services via Customer's Management Account or via Customer's access credentials and for all activity that occurs in Customer's Management Account. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Services or breach of its security relevant to the Hosted Services and will use commercially reasonable efforts to stop said breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

6. **Handling of Particular Information.** For the purposes of this ECSS Schedule, the definition of “Confidential Information” in the General Terms does not include any information that is Cloud Content (defined below), which is instead subject to this Section (Handling of Particular Information).

6.1. Administration Information. Entrust may store information in and related to Customer’s Order and Management Account and information generated by Customer’s usage of the Hosted Service, such as Customer’s access credentials, contact information for Agents, and entitlement consumption (“Administration Information”) in the United States and/or Canada, and may process Administration Information for the purposes of billing, providing Support and to investigate fraud, abuse or violations of this Agreement in the United States, Canada and other locations where Entrust maintains its support and investigation personnel.

6.2. Third Party Databases. In performing limited verification Entrust may determine whether the organizational identity, address, and domain name provided with a Certificate application are consistent with information contained in third-party databases (the "Databases"). Entrust may perform an investigation which may attempt to confirm certain Personal Data (as defined in the latest version of Entrust’s DPA) and other information, such as Customer’s business name, street address, mailing address, telephone number, line of business, year started, number of employees, CEO, telephone number and Customer’s business existence (collectively, “Verification Information”). Customer acknowledges that some of the Verification Information may become included in the Databases.

6.3. Certificate Information. Entrust may insert in a Certificate any information that is provided to Entrust in the associated application for the Certificate, which may include Verification Information (“Certificate Information”). Entrust may also (a) use such information that Customer provides to Entrust to authenticate Subscribers, (b) publish Customer’s Certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public, and (c) use such information for the purposes set out in the Agreement and in the Entrust Privacy Policy.

6.4. Cloud Content. “Cloud Content” means Administration Information, Verification Information, and Certificate Information, and any data, text or other content that Customer or any User transfers to Entrust for processing, storage or hosting by the Signing Services and any computational results that Customer or any User derives from the foregoing through its use of the Signing Service. Customer is aware and consents that Entrust will process and/or transfer the Cloud Content in North America and in any other jurisdictions where Entrust or any of its Affiliates maintains a presence, and may store Cloud Content in the cloud. Entrust may access and use the Cloud Content to provide the Hosted Services, or as necessary to comply with law or a binding order of a governmental body.

6.5. Cloud Risks. Although Cloud Content may be encrypted, Customer acknowledges that there are inherent risks in storing, transferring and otherwise processing data in the cloud, and that Entrust will have no liability to Customer for any unavailability of the Cloud Content, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Cloud Content or any data stored in, transferred to or from, or otherwise processed by the Hosted Services, including in transit.

6.6. Consents. Customer represents and warrants that Customer (and/or Users) has or will have obtained any requisite rights and consents, and made any requisite disclosures to relevant Users or other third parties, in accordance with all applicable laws, rules or regulations, to enable Customer and its Users to transfer the Cloud Content to Entrust. Customer hereby grants Entrust (including any of its applicable Affiliates, subcontractors or hosting service providers) all rights and consents required for the collection, use, and disclosure of the Cloud Content in accordance with the Agreement. Customer shall be responsible for the accuracy, quality and legality of Cloud Content and the means by which Customer acquired them.

6.7. Other Privacy Provisions. Except as otherwise provided in this Section (Handling of Particular Information) or in the Agreement, Entrust shall not disclose to any third party any Cloud Content that Entrust obtains in its performance of the Hosted Services hereunder. However, Entrust may make such information available (i) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Entrust’s legal counsel, (ii) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by Customer in the opinion of Entrust and (iii) to third parties as may be necessary for Entrust to perform its responsibilities under the Agreement.

7. **Software**. If Entrust provides any Software in connection with the Hosted Services, for example the Signing Automation Client in connection with a Signing Service, such Software is licensed under the terms of the Software Schedule attached hereto (and not this ECSS Schedule).

8. **Support Services**. Entrust provides the support commitments set out in the Support Schedule attached to this Schedule for the Hosted Services and any Software provided in connection with the Hosted Services. The "Silver Service Plan", as described in the Support Schedule, is included at no additional charge with a subscription to one or more of the Hosted Services. Other levels of Support may be available for purchase for an additional fee.

9. **Interoperability**. Entrust or third parties may make available plugins, agents or other tools that enable the Hosted Services to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Hosted Services, are licensed separately, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Services with such Interoperation Tools under this ECSS Schedule. If Customer uses any Interoperation Tool, Customer has exclusive responsibility to ensure that it has any and all requisite rights to use the Interoperation Tool, including using it to transfer any data from or to the Hosted Services, and to use the product or service with which it connects. The use of an Interoperation Tool does not create any data subprocessor relationship between Entrust and any third party.

10. **DISCLAIMER OF WARRANTY.** For the purposes of this ECSS Schedule, the following is added to the disclaimer of warranties in the General Terms: **Entrust makes no representations or warranties that any Certificate, Time-stamp or digital signature created using the Signing Services will be recognized or trusted by any particular third party or third party product or service.**

11. **INDEMNIFICATION.**

11.1. Additional Exception to IP Indemnity. In addition to the exceptions to indemnity in Section 10.1 (Intellectual Property Claims) of the General Terms, Entrust shall have no liability for any IP Claim in respect of any Certificate Services if the IP Claim arises from the technology that issued the certificate signing request (CSR) or any information contained in the CSR, unless the CSR was generated by Entrust.

11.2. Reserved

12. **LIABILITY.** In addition to, and without limiting the generality of, the liability limits and exclusions in the General Terms, the following specific exclusions also apply to the Hosted Services (for clarity, in this Section "Entrust" has the meaning in Section 11 (Liability) of the General Terms):

12.1. **SPECIFIC EXCLUSIONS. IN NO EVENT WILL ENTRUST BE LIABLE FOR, AND CUSTOMER WAIVES ANY RIGHT IT MAY HAVE TO, ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE, TIME-STAMP, THE CERTIFICATE SERVICES, OR TIME-STAMPING SERVICES PROVIDED UNDER THE AGREEMENT INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE, TIME-STAMP, CERTIFICATE SERVICES OR TIME-STAMPING SERVICES WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE, TIME-STAMP, CERTIFICATE SERVICES OR TIME-STAMPING SERVICES ALONE. FURTHER, IN NO EVENT WILL ENTRUST BE LIABLE FOR ANY DAMAGES TO SUBSCRIBERS, RELYING PARTIES OR ANY OTHER PERSON ARISING OUT OF OR RELATED TO THE USE OR MISUSE OF, OR RELIANCE ON ANY CERTIFICATE OR TIME-STAMP ISSUED UNDER THE AGREEMENT THAT: (I) HAS EXPIRED OR BEEN REVOKED; (II) HAS BEEN USED FOR ANY PURPOSE OTHER THAN AS SET FORTH IN THE AGREEMENT; (III) HAS BEEN TAMPERED WITH; (IV) WITH RESPECT TO WHICH THE KEY PAIR UNDERLYING SUCH CERTIFICATE OR THE CRYPTOGRAPHY ALGORITHM USED TO GENERATE SUCH CERTIFICATE'S KEY PAIR, HAS BEEN COMPROMISED BY THE ACTION OF ANY PARTY OTHER THAN ENTRUST (INCLUDING WITHOUT LIMITATION THE SUBSCRIBER OR RELYING PARTY); OR (V) IS THE SUBJECT OF MISREPRESENTATIONS OR OTHER MISLEADING ACTS OR OMISSIONS OF ANY OTHER PARTY, INCLUDING SUBSCRIBERS AND RELYING PARTIES. EXCEPT TO THE EXTENT EXPRESSLY PROVIDED IN THE AGREEMENT, IN NO EVENT SHALL ENTRUST BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR OTHER PARTY FOR DAMAGES ARISING OUT OF ANY CLAIM THAT THE CONTENT OF A CERTIFICATE (INCLUDING ANY VERIFIED MARKS IN A VMC) INFRINGES ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT OF ANY PARTY.**

13. Reserved

14. Offering Term and Termination.

14.1. Offering Term. The Certificate Services are sold either on a unit basis (per Certificate) or on a subscription basis. Signing Services and Dedicated CAs are sold on a subscription basis. The Offering Term will commence on the earliest of either the date that Entrust enables the Management Account for Customer's use, or the date that Customer is issued one or more Certificate(s). Unless otherwise specified on the Order, the Offering Term will continue in effect either: (i) for each Certificate purchased on a unit basis, for 365 days if the Certificate remains unissued, or for the validity period of the Certificate if it is issued; or (ii) for Hosted Services purchased on subscription basis, for the period stated in the Order. With respect to Time-stamping Services made available in connection with Certificate Services, the Offering Term will be the same as the Offering Term for the connected Certificate Services. In any case, the Offering Term may end earlier, upon termination of the Agreement in accordance with its terms.

14.2. Termination. In addition to the termination rights in the General Terms, the Agreement for the Hosted Services will terminate early in accordance with the procedures set forth in the Contract Disputes Act if Customer or its Users fail to comply with any of the material terms or conditions of this ECSS Schedule, the CPS or TPS, or upon revocation by Entrust of all Certificates issued hereunder if such revocation occurs prior to the end of the Offering Term. Entrust may also terminate the Agreement in in accordance with the procedures set forth in the Contract Disputes Act in order to comply with any third party licensing or other contractual or legal obligation (including any Industry Standard) to which Entrust is subject.

14.3. Effects of Termination or Expiry. Upon expiration of the Offering Term (unless succeeded immediately by a renewal Offering Term) or termination of the Agreement for a Hosted Service: (i) Customer must immediately cease all use of the Hosted Service; and (ii) Entrust may revoke all Certificates issued under the Agreement, and de-commission any Dedicated CAs.

15. Suspension. If, and to the extent that, Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including without limitation the security of other customers' (or their users') information or any other information or data processed by the Hosted Services, Entrust may, on written notice to the Customer, temporarily suspend provision of all or part of the applicable Hosted Services until such security concerns have been adequately addressed. Entrust must keep the Customer updated with the status of the security concerns.

16. Use of the Entrust Secured Site-Seal. Subject to the terms and conditions of the Agreement, Customer may use the Certificate Services with the Entrust Secured Site-Seal; provided, however that (i) Entrust delivers to Customer the Entrust Secured Site-Seal together with, or in conjunction with, the Certificate Services; and (ii) **BY EXECUTING A WRITTEN ORDER AND BY USING THE ENTRUST SECURED SITE-SEAL, CUSTOMER AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THE ENTRUST SECURED SITE-SEAL LICENSE AGREEMENT ATTACHED HERETO AND SET FORTH AT** http://www.entrust.net/cps**.**

17. Open Source Software and Third Party Products.

17.1. Open Source. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Offering ("Ancillary Software"). If a separate license agreement pertaining to Ancillary Software is embedded or provided with the Offerings, then the Ancillary Software is subject to the applicable separate license agreement pertaining to the Ancillary Software. Upon request, Entrust will provide Customer with a complete list of Ancillary Software and corresponding licenses, which list shall be deemed Entrust Confidential Information.

17.2. Third Party Products and Services. Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust through or in connection with the Hosted Services ("Third Party Vendor Products"). Except as expressly stated in this ECSS Schedule, Entrust has no obligation and excludes all liability with respect to Third Party Vendor Products, the use of which shall be exclusively subject to the applicable third party vendor's terms, conditions and policy documents ("Vendor Terms") accompanying, embedded in, or delivered with the Third Party Vendor Products or otherwise made available by the third party vendor. In particular:

17.2.1. If Customer purchases any Sixscape products (e.g. SixMail, SixEscrow) through Entrust or in connection with the Certificate Services, use of the Sixscape products shall be subject to the SixScape

Vendor Terms embedded in or delivered with the products and those which can be retrieved at www.sixscape.com/product-and-warranty/. Entrust shall provide support in relation to the Sixscape products pursuant to the Support Schedule attached hereto.

17.2.2. If Customer uses any WebID face-to-face verification Vendor Products, use of the WebID products shall be subject to the WebID Vendor Terms that must be accepted prior to accessing such products. Customer acknowledges and agrees that it will have the ability to submit Verification Information, including Personal Data, to WebID through the Management Account, and that WebID will deliver a data record package to Entrust to report verification results. For clarity, all processing by Entrust of Verification Information and Personal Data will be done in accordance with the Agreement, and processing by WebID will be done in accordance with the WebID Vendor Terms.

17.2.3. Entrust may make available, with certain Certificates, optional daily malware scanning services hosted by a Vendor on behalf of Entrust, as further described in the Documentation ("Malware Scanning Services"). Such Malware Scanning Services are subject to Customer supplying the information necessary to the Vendor to perform such services and accepting the Vendor Terms to receive the results. Entrust reserves the right to alter the features and functionality of the Malware Scanning Services or discontinue such services throughout the Offering Term and makes no warranty that any malware, security threats or vulnerabilities will be detected or is detectable by such services.

17.3. No Standalone Use. Any Third Party Vendor Product or Ancillary Software included with or embedded in the Offering may be used only with the applicable Offering, unless otherwise permitted in the applicable agreement accompanying such Third Party Vendor Product or Ancillary Software.

18. Reserved.

19. Publicity. During the Term and for thirty (30) days thereafter, Customer grants Entrust the right, free of charge, to use Customer's name to identify Customer as a customer on Entrust's website or other marketing or advertising materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

Exhibit A

Authorized to request a Certificate for Subscriber:	
Authorized to approve a request for a Certificate for Subscriber and to authorize others to request Certificates for Subscriber:	
Authorized to accept the subscriber agreement on Subscriber’s behalf:	

ENTRUST

Exhibit B

Representations, Warranties, and Obligations of Subscribers and Subjects

Part 1: Subscribers

As a condition of having any Certificate issued to or for Subscriber, each Subscriber makes, on its own behalf and if applicable on behalf of its principal or agent under a subcontractor or hosting service relationship, the following representations, commitments, affirmations and warranties for the benefit of Certificate Beneficiaries, Entrust and any of Entrust's Affiliates that will issue Certificates to or for Subscriber:

For all Certificates.

1. If Subscriber is applying for a Certificate to be issued to or for another Person, such Person has authorized Subscriber to act on its behalf, including to request Certificates on behalf of such Person, and to make the representations, commitments, affirmations and warranties in this Exhibit on behalf of such Person as well as on Subscriber's own behalf.
2. All information provided, and all representations made, at all times, by Subscriber in relation to any Certificate Services, including in the Certificate request and otherwise in connection with Certificate issuance, are and will be complete, correct and accurate (and such information and representations will be promptly updated from time to time as necessary to maintain such completeness, correctness and accuracy), and does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction. For clarity, in submitting any request for a Certificate using pre-qualified information, a Subscriber is deemed to be making anew the representations, commitments, affirmations and warranties set out in this Exhibit B, and Entrust will have no obligation to issue any Certificate containing pre-qualified information if such information is subsequently found to have changed or to be in any way inaccurate, incorrect, or misleading.
3. The private key corresponding to the public key submitted to Entrust with the Certificate request was created using sound cryptographic techniques and all reasonable measures have been taken to, at all times, assure control of (and, in the case of OV and EV code signing Certificates, sole control of), keep confidential, properly protect, and prohibit unauthorized use of, the private key (and any associated access or activation data or device, e.g., password or token), including, in the case of OV and EV code signing Certificates, in accordance with the "Data Security and Private Key Protection" provisions of the Code Signing BRs.
4. Any device storing private keys will be operated and maintained in a secure manner.
5. A Certificate will not be installed or used until Subscriber (or, in the case of code signing Certificates, Subscriber's Agent) has reviewed and verified that the content of the Certificate is accurate and correct.
6. In the case of all Entrust SSL Certificates, EV SSL Certificates and Private SSL Certificates, the Certificate will be installed only on servers that are accessible at the domain name (subjectAltName(s)) listed in the Certificate.
7. Certificates and the private key corresponding to the public key listed in such Certificate will only be used in compliance with all applicable laws and solely in accordance with the Agreement, and will only be used on behalf of the organization listed as the Subject in such Certificates.
8. The contents of Certificates will not be improperly modified.
9. Subscriber will notify Entrust, cease all use of the Certificate and the private key corresponding to the public key in the Certificate, and request the revocation of the Certificate,
   - 9.1. promptly, if any information included in the Certificate or the application for a Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
   - 9.2. immediately, if there is any actual or suspected loss, theft, misuse or compromise of the private key (or key activation data) corresponding to the public key in the Certificate, including if the value of the private key has been disclosed to an unauthorized person or an unauthorized person has had access to it ("**Key Compromise**"), or if control over the private key has been lost for other reasons.
   - 9.3. in the case of an OV or EV code signing Certificate, immediately, if there is evidence that the Certificate was used to sign Suspect Code.
10. Subscriber will promptly cease all use of the Certificate and the private key corresponding to the public key in such Certificate, upon expiration or revocation of such Certificate.
11. Subscriber will immediately respond to Entrust's instructions concerning any Key Compromise or misuse or suspected misuse of a Certificate.
12. Subscriber acknowledges and agrees that Entrust is entitled to revoke a Certificate immediately if:
    - 12.1. Customer breaches this Agreement.

12.2. Entrust discovers that there has been a Key Compromise of the Certificate's private key.
12.3. Revocation is required under the CPS or the Industry Standards.
12.4. Entrust discovers that the Certificate is compromised or being used for Suspect Code or the private key corresponding to the public key in the Certificate has been used to digitally sign Suspect Code.

13. Where the Subject named in the Certificate(s) is a separate entity from the Subscriber, the Subject has authorized the inclusion of the Subject's information in the Certificate.
14. Subscriber owns, controls, or has the exclusive right to use the domain name or email address listed in Certificate.
15. Subscriber acknowledges and agrees that Entrust is entitled to non-materially modify the Agreement when necessary to comply with any changes in Industry Standards.
16. Subscriber will use appropriate judgment about whether it is appropriate, given the level of security and trust provided by Certificate, to use the Certificate in any given circumstance.

Code Signing Certificates.

17. In addition, in the case of OV and EV code signing Certificates,

17.1. Subscriber will use commercially reasonable efforts to employ the code signing practices set out in the Code Signing Best Practices document attached hereto or by contacting Entrust ("**Code Signing Best Practices**").
17.2. Subscriber will generate and operate any device storing private keys in a secure manner, as described in the Code Signing Best Practices, and will use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
17.3. Subscriber will not request a code signing Certificate or EV code signing Certificate containing a public key that is, or will be used with any other type of Certificate.
17.4. The Certificate and the private key corresponding to the public key in such Certificate will only be used for authorized and legal purposes, and will not be used to digitally sign Suspect Code.
17.5. An adequate network and other security controls will be provided to protect against misuse of the private key corresponding to the public key in the Certificate.
17.6. Subscriber acknowledges and agrees that Entrust is authorized to share information about the Subscriber, signed application, Certificate, and surrounding circumstances with other certification authorities or industry groups, including the CA/Browser Forum, if:

17.6.1. the Certificate or Subscriber is identified as a source of Suspect Code,
17.6.2. the authority to request the Certificate cannot be verified, or
17.6.3. the Certificate is revoked for reasons other than at Subscriber's request (e.g. as a result of private key compromise, discovery of malware, etc.).

17.7. Subscriber acknowledges that ASVs may independently determine that a Certificate is malicious or compromised and that ASVs and ASV products may have the ability to modify its customer experiences or "blacklist" an OV or EV code signing Certificate without notice to Customer or Entrust and without regard to the revocation status of the code signing Certificate.

Qualified Certificates.

18. In addition, in the case of eIDAS QWACs, PSD2 QWACs, eIDAS QSealCs, PSD2 QSealCs, and eIDAS QSigCs,

18.1. Subscriber will comply with any requirements in the CPS for it to use a specific type of cryptographic device (including a secure cryptographic device or a qualified electronic signature/seal creation device "QSCD"), and if so required:

18.1.1. the Subject's private key(s) will only be used for cryptographic functions within the specified cryptographic device.
18.1.2. if the Subject's keys are generated under control of the Subscriber or Subject, the Subject's keys will be generated within the specified cryptographic device.

18.2. Subscriber consents to Entrust's keeping of a record of information used in registration, subject device provision, including whether this is to the Subscriber or to the Subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required by Industry Standards in the case of Entrust terminating its services.

18.3. Subscriber requires the publication of the Certificate in the manner and in accordance with the conditions set out in the CPS and will obtain, where applicable, the Subject’s consent to such publication.
18.4. The private key and corresponding public key associated with the Certificate will only be used in accordance with the limitations notified to the Subscriber, including in the CPS.
18.5. If the Subscriber or Subject generates the Subject's keys:
18.5.1. the Subject keys will be generated using an algorithm as specified in the Industry Standards for the uses of the certified key as identified in the CPS.
18.5.2. the key length and algorithm will be as specified in the Industry Standards for the uses of the certified key as identified in the CPS during the validity time of the Certificate.
18.5.3. the Subject’s Private Key will be maintained under the Subject’s control, and, if the Subject is an individual, the Subject's sole control.
18.6. The Subject's private key will be used under the Subject's control, and, if the Subject is an individual, the Subject’s sole control.
18.7. Upon being informed that the Subject’s Certificate has been revoked, or that the issuing CA has been compromised, Subscriber will ensure that the private key corresponding to the public key in the Certificate is no longer used by the Subject.
18.8. In respect to eIDAS QSigC, key pairs will only be used for electronic signatures.
18.9. In respect to eIDAS QSealC and PSD2 QSealC, key pairs will only be used for electronic seals.

Verified Mark Certificates.

19. In addition, in the case of VMCs:
19.1. Subscriber will apply for and use VMCs in accordance with and subject to the VMC Requirements.
19.2. The trademarks submitted in a VMC application represent registered trademarks that the Subscriber owns or for which it has obtained sufficient license to be able to grant the limited license in the Terms of Use attached to the VMC Requirements, and that it will immediately revoke the VMC if it no longer owns or has a sufficient license to the applicable trademarks.

Part 2: Individual Subjects, when different from the Subscriber

If the Subject and Subscriber are separate entities and the Subject is a Person (i.e. not a device), as a condition of having any eIDAS QWAC, PSD2 QWAC, eIDAS QSealC, PSD2 QSealC and eIDAS QSigC issued to or for it, the Subject accepts the following obligations:

1. Subject will comply with any requirements in the CPS for it to use a specific type of cryptographic device (including a secure cryptographic device or QSCD), and if so required, the Subject’s private key(s) will only be used for cryptographic functions with the specified cryptographic device.
2. Subject consents to Entrust’s keeping of a record of information used in registration, subject device provision, including whether this is to the Subscriber or to the Subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required by ETSI EN 319 411-1 in the case of Entrust terminating its services.
3. Private key and corresponding public key associated with the Certificate will only be used in accordance with the limitations notified to the Subject, including in the CPS.
4. Subject will prohibit unauthorized use of the Subject's private key.
5. If the Subject generates the Subject's keys, the Subject's private key will be maintained under the Subject's control, and, if the Subject is an individual, the Subject’s sole control.
6. The Subject's private key will be used under the Subject's control, and, if the Subject is an individual, the Subject’s sole control.
7. Subject will notify Entrust immediately:
7.1. if any information included in the Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
7.2. and immediately and permanently discontinue use of the applicable key, if there is any actual or suspected loss, theft, misuse or compromise of the private key (or key activation data) corresponding to the public key in the Certificate, including if the value of the private key has been disclosed to an unauthorized person or an unauthorized person has had access to it, or if control over the private key has been lost for other reasons.

8. Upon being informed that the Subject’s Certificate has been revoked, or that the issuing CA has been compromised, Subject will no longer use the private key.

ENTRUST

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope.**

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery.** Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty.**

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination.**

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users.** Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source**. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms")**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. "**Business Day**" means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. "**Covered Offering**" means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. "**Customer-Hosted Offering**" means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer's premises.

1.4. "**Extended Support**" means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. "**Hosted Service**" for the purposes of this Schedule means Entrust's Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. "**Incident**" means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. "**Named Support Contacts**" means individual Users nominated by Customer to act as Customer's support representatives.

1.8. "**Problem**" means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. "**Production Environment**" means Customer's live business environment with active users.

1.10. "**Response Time**" means the amount of time that elapses between the Customer's report of a Service Request to Entrust and Entrust's acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. "**Service Plan**" means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**" means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. "**Software**" for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. "**Superseded Product**" means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain

additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees**.

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer's Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail ("Immediate Incident Response Time").

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. <u>Upgrades for Customer-Hosted Offerings</u>.

8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions.**

9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with contract Disputes Clause (Contract Disputes Act).

Code Signing Best Practices

Code Signing Best Practices

The biggest issue with code signing is the protection of the private signing key associated with the code signing certificate. If a key is compromised, the certificate loses trust and value, jeopardizing the software that you have already signed.

Consider the following code signing best practices:

1. Minimize access to private keys
   - Allow minimal connections to computers with keys
   - Minimize the number of users who have key access
   - Use physical security controls to reduce access to keys

2. Protect private keys with cryptographic hardware products
   - Cryptographic hardware does not allow export of the private key to software where it could be attacked
   - Use a FIPS 140 Level 2-certified product (or better)
   - If private keys will be transported, ensure the cryptographic hardware is protected with a randomly generated password of at least 16 characters which contains uppercase letters, lowercase letters, numbers and special characters

3. Time-stamp code
   - Time-stamping allows code to be verified after the certificate has expired or been revoked
   - Time-stamp certificates can be issued for a maximum of 135 months which can support the signed software to be validated for up to 11 years

4. Understand the difference between test-signing and release-signing
   - Test-signing private keys and certificates requires less security access controls than production code signing private keys and certificates
   - Test-signing certificates can be self-signed or come from an internal test CA
   - Test certificates must chain to a completely different root certificate than the root certificate that is used to sign publicly released products; this precaution helps ensure that test certificates are trusted only within the intended test environment
   - Establish a separate test code signing infrastructure to test-sign pre-release builds of software

5. Authenticate code to be signed
   - Any code that is submitted for signing should be strongly authenticated before it is signed and released
   - Implement a code signing submission and approval process to prevent the signing of unapproved or malicious code
   - Log all code signing activities for auditing and/or incident-response purposes

6. Virus scan code before signing
   - Code signing does not confirm the safety or quality of the code; it confirms the publisher and whether or not the code has been changed
   - Take care when incorporating code from other sources
   - Implement virus-scanning to help improve the quality of the released code

7. Do not over-use any one key (distribute risk with multiple certificates)
    - If code is found with a security flaw, then publishers may want to prompt a User Account Control dialogue box to appear when the code is installed in the future; this can be done by revoking the code signing certificate so a revoked prompt will occur
    - If the code with the security flaw was issued before more good code was issued, then revoking the certificate will impact the good code as well
    - Changing keys and certificates often will help to avoid this conflict

8. Revoking compromised certificates
    - Report key compromise or signed malware to your certification authority
    - Compromised keys or signed malware of suspect code will require the code signing certificate to be revoked
    - Assuming that all signed code has been time-stamped, then the revocation date can be selected before the time of compromise. This will mean that code signed before the revocation date may not be impacted.

References

The following references will support Windows and Java code signing.

- Guide to Code Signing for Authenticode
- Guide to Code Signing for Java
- Guide to Code Signing for Windows Macros & Visual Basic
- Guide to Code Signing and EV Code Signing Certificate for Download and Installation

ENTRUST

Certificate and Signing Services
Terms of Use

The Agreement for Entrust's Certificate Services, any digital Signing Services, Time-stamping Services and/or Dedicated CAs is made up of these terms of use (the "ECSS Schedule"), the CPS and/or TPS (each defined below), the Entrust General Terms and Conditions ("General Terms") and an Order for Certificate Services, Signing Services, and/or Dedicated CAs. Capitalized terms not defined herein have the meanings given to them in the General Terms.

For clarity, the parties acknowledge and agree that the Agreement as defined above constitutes the subscriber agreement, as required and defined in the Industry Standards, for all Certificates issued hereunder.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE HOSTED SERVICES. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICES IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. Definitions.

1.1. "**Application Software Vendor**" or "**ASV**" means a developer of Internet browser software, email software or other software that displays or uses Certificates, including but not limited to Adobe, Apple, Google, Intel, Microsoft, Mozilla, and Oracle.

1.2. "**Certificate**" means a digital document that at a minimum: (a) identifies the certification authority issuing it, (b) names or otherwise identifies a Subject; (c) contains a public key of a key pair, (d) identifies its operational period, (e) contains a serial number and (f) is digitally signed by the certification authority. There are various types of Certificate(s) that may be issued to Subscriber by Entrust depending upon the Certificate Services that have been purchased, for example (and not exhaustively) OV SSL Certificates, extended validation ("**EV**") SSL Certificates, OV code signing Certificates, EV code signing Certificates, document signing Certificates, verified mark Certificates ("**VMC**s"), mobile device Certificates, private SSL Certificates, SMIME Certificates, eIDAS qualified website authentication Certificates ("**eIDAS QWAC**s"), PSD2 qualified website authentication Certificates ("**PSD2 QWAC**s"), eIDAS qualified seal certificate(s) ("**eIDAS QSealCs**"), PSD2 qualified Seal Certificate(s) ("**PSD2 QSealCs**"), and eIDAS Qualified Signature Certificate(s) ("**eIDAS QSigCs**").

1.3. "**Certificate Beneficiaries**" means, collectively, all Application Software Vendors with whom Entrust has entered into a contract to include Entrust's root Certificate(s) in such ASV's software, and all Relying Parties that actually rely on such Certificate during the period when it is Valid.

1.4. "**Certificate Services**" means the services offered by Entrust relating to the issuance, management and revocation of one or more Certificate(s), including Foreign Certificate Management Right(s), and includes any Certificate(s) issued to or for Customer pursuant to the Agreement.

1.5. "**CPS**" means the most recent version of the certification practice statement that is incorporated by reference into the Certificate(s) that are issued by Entrust, as may be amended from time to time in accordance with the terms of the CPS, and which is also hereby incorporated by reference into the Agreement. The CPS applicable to a specific Certificate depends on the type of Certificate and can be found on the Internet at http://www.entrust.net/cps or by contacting Entrust. For example, eIDAS QWACs and PSD2 QWACs are governed by the most recent version of the document titled "Certification Practice Statement For Qualified Certificates", private SSL Certificate(s) are governed by the most recent version of the document titled "Certification Practice Statement For Private Trust Certificates", and other Certificates are generally governed by the most recent version of the document titled "Certification Practice Statement".

1.6. “**Dedicated CA**” means an issuing certification authority chaining up to one of Entrust’s public root CAs dedicated to issuing Certificates for Customer.

1.7. “**Foreign Certificate(s)**” means any Certificate that was not issued to or for Customer under this ECSS Schedule. For greater certainty, Foreign Certificates may include, but are not limited to, Certificates issued from other management services accounts, Certificates purchased from Entrust’s retail web site, Certificates issued from other Entrust service offerings (for example, PKI as a Service), and Certificates issued by any third party.

1.8. “**Foreign Certificate Management Right(s)**” means an optional license enabling Customer to use its Management Account to receive certain management services (as set out in the Documentation) for one (1) Foreign Certificate for each Foreign Certificate Management Right(s) purchased by Customer. The quantity of Foreign Certificate Management Right(s) available to Customer will be tracked by its Management Account and Customer’s inventory of available Foreign Certificate Management Right(s) will be increased or decreased by a quantity corresponding to the number of Foreign Certificates added to or released from its Management Account.

1.9. “**Hosted Services**” means, in this ECSS Schedule, the specific Certificate Services and any Time-stamping Services, Signing Services and/or Dedicated CAs that Customer has purchased as specified in the Order, and includes a Management Account.

1.10. “**Industry Standards**” means, collectively, the most up-to-date versions of each of the following, in each case, that are applicable to the various types of publicly-trusted Certificates and Time-stamps issued by Entrust, and to which Entrust is subject and bound as an issuer of such Certificates and Time-stamps:

1.10.1. the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,

1.10.2. the CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Certificates (“EV Guidelines”),

1.10.3. the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates (“Code Signing BRs”),

1.10.4. European Standards produced by the ETSI Technical Committee Electronic Signatures and Infrastructures,

1.10.5. the Minimum Security Requirements for Issuance of Verified Mark Certificates approved by the Authindicators Working Group for VMCs (“VMC Requirements”), and

1.10.6. laws and regulations.

1.11. “**Management Account**” means a self-service administration tool hosted by Entrust that identifies Customer by its full legal name in the “Customer Name” field, tracks Customer’s entitlements with respect to the Hosted Services and enables Customer, as applicable in accordance with its entitlements, to manage the issuance, revocation, and expiry of one or more Certificate(s) and access and use the Signing Services.

1.12. “**Relying Party**” means any individual or entity that relies on a Valid Certificate or on a Time-Stamp. For avoidance of doubt, an ASV is not a “Relying Party” when software distributed by such ASV merely displays information regarding a Certificate.

1.13. **“Signing Services”** means the services offered by Entrust relating to the generation, management and hosting of keys to sign hashed data.

1.14. “**Subject**” means the Person or device identified in the “Subject” field in a Certificate.

1.15. “**Subscriber**” means the Person who applies for or is issued a Certificate.

1.16. “**Suspect Code**” means any code or set of instructions that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the computing environment on which it executes.

1.17. “**Time-stamp**” means data in electronic form which binds other electronic data to a particular time establishing evidence that these data existed at that time.

1.18. “**Time-stamping Services**” means the services offered by Entrust relating to the issuance of one or more Time-stamp(s), and includes any Time-stamp(s) issued to or for Customer pursuant to the Agreement.

1.19. “**TPS**” means the most recent version of the timestamping practice statement describing the practices followed by Entrust in issuing Time-stamp(s), as may be amended from time to time in accordance with the terms of the TPS, and which is also hereby incorporated by reference into the Agreement. The TPS applicable to a specific Time-stamp depends on the type of Time-stamp and can be found on the Internet at http://www.entrust.net/cps or by contacting Entrust.

1.20. “**Users**” has the meaning set out in the General Terms, and in this ECSS Schedule, includes Customer’s Agents and all Persons who are Subjects and Subscribers of Certificates and Time-stamps issued using Customer’s Management Account.

1.21. “**Valid**” means that a Certificate has not expired and has not been revoked.

2. Operation of the PKI. Each CPS and TPS sets out Entrust’s practices for managing the public-key infrastructure for the Hosted Services and providing the types of Certificates identified in the CPS and Time-stamps identified in the TPS, including:

(a) Specification of the applicable Industry Standards and policies;
(b) Information for Relying Parties;
(c) Event log retention period;
(d) Procedures for complaints and dispute settlement;
(e) Specification of the applicable compliance audits and other assessments;
(f) Contact information for questions about Certificates and Time-stamps;
(g) How revocation status information is provided and the period over which it is available.

3. Hosted Services Details. Provision of Hosted Services. Entrust will generate, provide and operate the Hosted Services in accordance with the applicable CPS, TPS, Documentation, and Customer’s Order(s) for the Hosted Services. Without limiting the foregoing:

3.1. Certificate Services—Verification, Issuance and Revocation of Certificate(s). Upon receipt of an application for a Certificate, Entrust will perform the limited verification of the information contained in the application as described in the CPS for the applicable type of Certificate. After completing such verification, Entrust will issue Certificate(s) and make them available for retrieval and management if and as set out in the CPS, the Documentation, and Customer’s entitlements under its Order for Certificate Services. Entrust may reject applications for Certificates for the reasons set out in the CPS. Entrust is entitled to revoke a Certificate it has issued if revocation is requested by Customer, upon expiry or termination of the Agreement, or for any other reason identified for revocation in the Agreement, the CPS or the Industry Standards.

3.2. Signing Services. Upon receipt of a request for key generation, Entrust will generate and host a key pair, and make the keys available for Customer’s use in connection with a Certificate for which Customer or one of its Affiliates is the Subscriber and/or the Subject, all if and as set out in the CPS, the Documentation, and Customer’s entitlements under its Order for Signing Services.

3.3. Time-stamping Services. Upon receipt of a request for a Time-stamp, Entrust will issue a Time-stamp, all if and as set out in the TPS, the Documentation, and Customer’s entitlements under its Order for Time-stamping Services.

3.4. Dedicated CA. If an Order calls for one or more Dedicated CA(s) to be provided for Customer’s use, Entrust will host and operate each Dedicated CA in accordance with the CPS, Documentation, and Customer’s entitlements under its Order for the Dedicated CA. The details of the Dedicated CA, such as the Subject to be identified in the Dedicated CA Certificate, the types of Certificate that will be issued by the Dedicated CA, and any other limitations or requirements, will be specified in a written addendum mutually executed by the parties, or in the Order for the Dedicated CA. Any Dedicated CA addendum is hereby included in the “Agreement” for the Dedicated CA. The Dedicated CA and its keys will be owned and controlled by Entrust. The validity period of the CA Certificate for a Dedicated CA will be no longer than that of the root CA that issued it, but may be revoked by Entrust if revocation is requested by Customer, upon expiry or termination of the Offering Term, or for any other reason identified for revocation in the Agreement, the CPS or the Industry Standards.

3.5. Hosted Service Revisions. Entrust may modify Hosted Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to a Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice on Entrust's website constitutes written notice).

4. Grant of Rights.

4.1. General Use. Subject to Customer (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Services, and to grant its Users the ability to access and use the Hosted Services, and to distribute Certificates issued by the Certificate Services, in each case solely (a) in accordance with this ECSS Schedule and the CPS and/or TPS, as applicable; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Hosted Services that Customer is permitted to use, such as limits associated with subscription types or levels, and on numbers or types of Certificates, Time-stamps, identities, Users, signatures or devices purchased; and (d) subject to the general restrictions set out in Section 3 of the General Terms (Restrictions).

4.2. Evaluation Use. At Entrust's discretion, it may provide Customer with access to and right to use any of the Hosted Services for evaluation purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Section 4.2 (Evaluation Use) or a separate evaluation agreement executed by the parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms, this ECSS Schedule, the CPS and/or TPS, as applicable, and an applicable Order (if any), for sixty (60) days Customer may, solely as necessary for Customer's evaluation of a Hosted Service, access and use the Hosted Service exclusively in, from and/or in connection with a Customer test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data). For clarity, Certificates issued in connection with an evaluation of Certificate Services ("Trial Certificates") shall have a maximum operational period of 60 days and may not be used for production purposes. Performance and security testing is expressly excluded from evaluation purposes and is strictly prohibited. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 4.1 (General Use), 8 (Support Services), 14.1 (Offering Term) and 19 (Publicity) do not apply to any evaluation of the Hosted Service. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Service at any time, for any or no reason, without advance notice. Customer will revoke any and all outstanding Trial Certificates when Customer has completed the evaluation but in all cases prior to the termination of the evaluation period or any trial account created for the evaluation. Customer hereby authorizes Entrust to revoke any and all outstanding Trial Certificates upon the termination of the evaluation period or any trial account created for the evaluation.

5. Customer Roles, Responsibilities, and Representations and Warranties.

5.1. Agents. A Subscriber may exercise its rights and obligations with respect to the Certificate Services through Customer or through certain Users appointed to fulfill the roles set out in Exhibit A, subject to any applicable verification or confirmation requirements set out in the CPS, such as verification that a person requesting EV Certificates is a verified 'Certificate Requester' under the EV Guidelines ("Agents"). The appointed Agents may be identified in Exhibit A, or will be provided to Entrust during enrollment. Such appointment may be modified using means established by Entrust from time to time. Subscriber agrees that Entrust is entitled to rely on instructions provided by the Agents with respect to the Hosted Services as if such instructions were provided by the Subscriber itself.

5.2. Signing Service Users. Customer may exercise its rights and obligations with respect to the Signing Services through certain Users appointed by Customer in its discretion ("**Signing Service Users**"). Such appointment may be modified using means established by Entrust from time to time. Customer agrees that it is responsible for Signing Service Users' compliance with the Agreement and for the Signing Service Users' use of the keys hosted by the Signing Services.

5.3. Representations and Warranties. Customer will comply with the requirements set forth in Exhibit B as applicable to Customer when it acts in the capacity of Subscriber or Subject. Customer will notify all Customer Affiliates, Users and any other Persons who act in the capacity of Subscriber, Subject, Agent or

Signing Service User (e.g. apply for, receive, are issued, or manage Certificates, or use Signing Services to generate keys and/or sign hashed data) under this ECSS Schedule through Customer's Management Account that they are required to comply with the requirements set forth in this Agreement (including those set out in Exhibit B) as applicable to the activities and roles of Subscribers, Subjects, Agents and Signing Service Users in connection with the Hosted Services and Certificates, and Customer will be responsible for ensuring such compliance. Customer represents and warrants to Entrust and all Certificate Beneficiaries that Customer has the authority to bind all Subscribers to the Agreement if and to the extent that such Subscribers are issued any Certificate(s) under this ECSS Schedule through Customer's Management Account. Customer represents and warrants that each of its Signing Service Users has or will have obtained any requisite rights and authorizations for Signing Service Users' use of the keys hosted by the Signing Services.

5.4. Separate Subjects. For certain Certificates, as permitted by the applicable CPS, e.g. mobile device Certificates, SMIME Certificates, and certain document signing Certificates ("Client Certificates"), the Subject of the Certificate may be an individual who is different from the Subscriber. If Customer's Order entitles it to any Client Certificates, Customer agrees that such Client Certificates will only be issued and distributed to such Subjects pursuant to the most recent version of the Client Certificate Agreement that can be found at http://www.entrust.net/cps and provided that (i) Subscriber has verified the information included in each Client Certificate as being accurate; (ii) the individual to whom such Client Certificate is issued has consented to the inclusion of all data that is incorporated into such Client Certificates; (iii) the individual to whom such Client Certificate is issued has been notified of its obligations pursuant to Section 5.3 (Representations and Warranties) above and (iv) such Client Certificate is used only for Subscriber-related business.

5.5. Customer-hosted Components. If Customer's Order for a Hosted Service includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Service (collectively, "Customer-hosted Products"), Customer will be responsible for the lifecycle management (patching, upgrades, etc.) of such Customer-hosted Products and the security of the environment where it installs and uses such Customer-hosted Products. Customer will implement commercially reasonable security measures with respect to the Customer-hosted Products and the environment where they are installed. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures; and (ii) for any Customer-hosted Products that are or include software, always use the current version of such software and promptly install any security patches and any upgrades/updates required for proper functioning of all features of the Hosted Service. Customer understands if it fails to comply with this Section it could create a security risk and/or otherwise negatively impact the operation of the Hosted Service and Entrust may have the right to suspend the Hosted Service in accordance with Section 15 (Suspension). In addition, Customer may not be able to access new features or functions of the Hosted Service if it does not comply with this Section.

5.6. Network Requirements. Customer is responsible for procuring, maintaining, monitoring and supporting its communications infrastructure, network (LAN or WAN), and all components that connect to the Hosted Service(s). Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure, nor for any service degradation or failures caused by network connectivity of such external infrastructure.

5.7. Devices. For Certificates issued to devices, Customer is responsible for ensuring that the relevant devices support and are interoperable with the Certificates.

5.8. Unauthorized Access. Customer will take all reasonable steps to prevent unauthorized access to the Hosted Services, including by securing, protecting and maintaining the confidentiality of its access credentials. Customer is responsible for any access and use of the Hosted Services via Customer's Management Account or via Customer's access credentials and for all activity that occurs in Customer's Management Account. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Services or breach of its security relevant to the Hosted Services and will use commercially reasonable efforts to stop said breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

6. **Handling of Particular Information.** For the purposes of this ECSS Schedule, the definition of "Confidential Information" in the General Terms does not include any information that is Cloud Content (defined below), which is instead subject to this Section (Handling of Particular Information).

6.1. Administration Information. Entrust may store information in and related to Customer's Order and Management Account and information generated by Customer's usage of the Hosted Service, such as Customer's access credentials, contact information for Agents, and entitlement consumption ("Administration Information") in the United States and/or Canada, and may process Administration Information for the purposes of billing, providing Support and to investigate fraud, abuse or violations of this Agreement in the United States, Canada and other locations where Entrust maintains its support and investigation personnel.

6.2. Third Party Databases. In performing limited verification Entrust may determine whether the organizational identity, address, and domain name provided with a Certificate application are consistent with information contained in third-party databases (the "Databases"). Entrust may perform an investigation which may attempt to confirm certain Personal Data (as defined in the latest version of Entrust's DPA) and other information, such as Customer's business name, street address, mailing address, telephone number, line of business, year started, number of employees, CEO, telephone number and Customer's business existence (collectively, "Verification Information"). Customer acknowledges that some of the Verification Information may become included in the Databases.

6.3. Certificate Information. Entrust may insert in a Certificate any information that is provided to Entrust in the associated application for the Certificate, which may include Verification Information ("Certificate Information"). Entrust may also (a) use such information that Customer provides to Entrust to authenticate Subscribers, (b) publish Customer's Certificates to one or more CT (Certificate Transparency) logs which may be viewed by the public, and (c) use such information for the purposes set out in the Agreement and in the Entrust Privacy Policy.

6.4. Cloud Content. "Cloud Content" means Administration Information, Verification Information, and Certificate Information, and any data, text or other content that Customer or any User transfers to Entrust for processing, storage or hosting by the Signing Services and any computational results that Customer or any User derives from the foregoing through its use of the Signing Service. Customer is aware and consents that Entrust will process and/or transfer the Cloud Content in North America and in any other jurisdictions where Entrust or any of its Affiliates maintains a presence, and may store Cloud Content in the cloud. Entrust may access and use the Cloud Content to provide the Hosted Services, or as necessary to comply with law or a binding order of a governmental body.

6.5. Cloud Risks. Although Cloud Content may be encrypted, Customer acknowledges that there are inherent risks in storing, transferring and otherwise processing data in the cloud, and that Entrust will have no liability to Customer for any unavailability of the Cloud Content, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Cloud Content or any data stored in, transferred to or from, or otherwise processed by the Hosted Services, including in transit.

6.6. Consents. Customer represents and warrants that Customer (and/or Users) has or will have obtained any requisite rights and consents, and made any requisite disclosures to relevant Users or other third parties, in accordance with all applicable laws, rules or regulations, to enable Customer and its Users to transfer the Cloud Content to Entrust. Customer hereby grants Entrust (including any of its applicable Affiliates, subcontractors or hosting service providers) all rights and consents required for the collection, use, and disclosure of the Cloud Content in accordance with the Agreement. Customer shall be responsible for the accuracy, quality and legality of Cloud Content and the means by which Customer acquired them.

6.7. Other Privacy Provisions. Except as otherwise provided in this Section (Handling of Particular Information) or in the Agreement, Entrust shall not disclose to any third party any Cloud Content that Entrust obtains in its performance of the Hosted Services hereunder. However, Entrust may make such information available (i) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Entrust's legal counsel, (ii) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by Customer in the opinion of Entrust and (iii) to third parties as may be necessary for Entrust to perform its responsibilities under the Agreement.

7. **Software**. If Entrust provides any Software in connection with the Hosted Services, for example the Signing Automation Client in connection with a Signing Service, such Software is licensed under the terms of the Software Schedule attached hereto (and not this ECSS Schedule).

8. **Support Services**. Entrust provides the support commitments set out in the Support Schedule attached hereto for the Hosted Services and any Software provided in connection with the Hosted Services. The "Silver Service

Plan", as described in the Support Schedule, is included at no additional charge with a subscription to one or more of the Hosted Services. Other levels of Support may be available for purchase for an additional fee.

9. **Interoperability**. Entrust or third parties may make available plugins, agents or other tools that enable the Hosted Services to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Hosted Services, are licensed separately, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Services with such Interoperation Tools under this ECSS Schedule. If Customer uses any Interoperation Tool, Customer has exclusive responsibility to ensure that it has any and all requisite rights to use the Interoperation Tool, including using it to transfer any data from or to the Hosted Services, and to use the product or service with which it connects. The use of an Interoperation Tool does not create any data subprocessor relationship between Entrust and any third party.

10. **DISCLAIMER OF WARRANTY.** For the purposes of this ECSS Schedule, the following is added to the disclaimer of warranties in the General Terms: **Entrust makes no representations or warranties that any Certificate, Time-stamp or digital signature created using the Signing Services will be recognized or trusted by any particular third party or third party product or service.**

11. **INDEMNIFICATION.**

11.1. Additional Exception to IP Indemnity. In addition to the exceptions to indemnity in Section 10.1 (Intellectual Property Claims) of the General Terms, Entrust shall have no liability for any IP Claim in respect of any Certificate Services if the IP Claim arises from the technology that issued the certificate signing request (CSR) or any information contained in the CSR, unless the CSR was generated by Entrust.

11.2. Reserved

12. **LIABILITY.** In addition to, and without limiting the generality of, the liability limits and exclusions in the General Terms, the following specific exclusions also apply to the Hosted Services (for clarity, in this Section "Entrust" has the meaning in Section 11 (Liability) of the General Terms):

12.1. **SPECIFIC EXCLUSIONS. IN NO EVENT WILL ENTRUST BE LIABLE FOR, AND CUSTOMER WAIVES ANY RIGHT IT MAY HAVE TO, ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE, TIME-STAMP, THE CERTIFICATE SERVICES, OR TIME-STAMPING SERVICES PROVIDED UNDER THE AGREEMENT INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE, TIME-STAMP, CERTIFICATE SERVICES OR TIME-STAMPING SERVICES WITH ANY SOFTWARE OR HARDWARE NOT PROVIDED BY ENTRUST IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE, TIME-STAMP, CERTIFICATE SERVICES OR TIME-STAMPING SERVICES ALONE. FURTHER, IN NO EVENT WILL ENTRUST BE LIABLE FOR ANY DAMAGES TO SUBSCRIBERS, RELYING PARTIES OR ANY OTHER PERSON ARISING OUT OF OR RELATED TO THE USE OR MISUSE OF, OR RELIANCE ON ANY CERTIFICATE OR TIME-STAMP ISSUED UNDER THE AGREEMENT THAT: (I) HAS EXPIRED OR BEEN REVOKED; (II) HAS BEEN USED FOR ANY PURPOSE OTHER THAN AS SET FORTH IN THE AGREEMENT; (III) HAS BEEN TAMPERED WITH; (IV) WITH RESPECT TO WHICH THE KEY PAIR UNDERLYING SUCH CERTIFICATE OR THE CRYPTOGRAPHY ALGORITHM USED TO GENERATE SUCH CERTIFICATE'S KEY PAIR, HAS BEEN COMPROMISED BY THE ACTION OF ANY PARTY OTHER THAN ENTRUST (INCLUDING WITHOUT LIMITATION THE SUBSCRIBER OR RELYING PARTY); OR (V) IS THE SUBJECT OF MISREPRESENTATIONS OR OTHER MISLEADING ACTS OR OMISSIONS OF ANY OTHER PARTY, INCLUDING SUBSCRIBERS AND RELYING PARTIES. EXCEPT TO THE EXTENT EXPRESSLY PROVIDED IN THE AGREEMENT, IN NO EVENT SHALL ENTRUST BE LIABLE TO THE SUBSCRIBER, RELYING PARTY OR OTHER PARTY FOR DAMAGES ARISING OUT OF ANY CLAIM THAT THE CONTENT OF A CERTIFICATE (INCLUDING ANY VERIFIED MARKS IN A VMC) INFRINGES ANY PATENT, TRADEMARK, COPYRIGHT, TRADE SECRET OR OTHER INTELLECTUAL PROPERTY RIGHT OF ANY PARTY.**

13. **Reserved**

14. **Offering Term and Termination.**

14.1. Offering Term. The Certificate Services are sold either on a unit basis (per Certificate) or on a subscription basis. Signing Services and Dedicated CAs are sold on a subscription basis. The Offering Term will commence on the earliest of either the date that Entrust enables the Management Account for Customer's use, or the date that Customer is issued one or more Certificate(s). Unless otherwise specified on the Order, the Offering Term will continue in effect either: (i) for each Certificate purchased on a unit basis, for 365 days if the Certificate remains unissued, or for the validity period of the Certificate if it is issued; or (ii) for Hosted Services purchased on subscription basis, for the period stated in the Order. With respect to Time-stamping Services made available in connection with Certificate Services, the Offering Term will be the same as the Offering Term for the connected Certificate Services. In any case, the Offering Term may end earlier, upon termination of the Agreement in accordance with its terms.

14.2. Termination. In addition to the termination rights in the General Terms, the Agreement for the Hosted Services will terminate early in accordance with the procedures set forth in the Contract Disputes Act if Customer or its Users fail to comply with any of the material terms or conditions of this ECSS Schedule, the CPS or TPS, or upon revocation by Entrust of all Certificates issued hereunder if such revocation occurs prior to the end of the Offering Term. Entrust may also terminate the Agreement in in accordance with the procedures set forth in the Contract Disputes Act in order to comply with any third party licensing or other contractual or legal obligation (including any Industry Standard) to which Entrust is subject.

14.3. Effects of Termination or Expiry. Upon expiration of the Offering Term (unless succeeded immediately by a renewal Offering Term) or termination of the Agreement for a Hosted Service: (i) Customer must immediately cease all use of the Hosted Service; and (ii) Entrust may revoke all Certificates issued under the Agreement, and de-commission any Dedicated CAs.

15. Suspension. If, and to the extent that, Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including without limitation the security of other customers' (or their users') information or any other information or data processed by the Hosted Services, Entrust may, on written notice to the Customer, temporarily suspend provision of all or part of the applicable Hosted Services until such security concerns have been adequately addressed. Entrust must keep the Customer updated with the status of the security concerns.

16. Use of the Entrust Secured Site-Seal. Subject to the terms and conditions of the Agreement, Customer may use the Certificate Services with the Entrust Secured Site-Seal; provided, however that (i) Entrust delivers to Customer the Entrust Secured Site-Seal together with, or in conjunction with, the Certificate Services; and (ii) **BY EXECUTING A WRITTEN ORDER AND BY USING THE ENTRUST SECURED SITE-SEAL, CUSTOMER AGREES TO BE BOUND BY THE TERMS AND CONDITIONS OF THE ENTRUST SECURED SITE-SEAL LICENSE AGREEMENT ATTACHED HERETO AND SET FORTH AT** http://www.entrust.net/cps**.**

17. Open Source Software and Third Party Products.

17.1. Open Source. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Offering ("Ancillary Software"). If a separate license agreement pertaining to Ancillary Software is embedded or provided with the Offerings, then the Ancillary Software is subject to the applicable separate license agreement pertaining to the Ancillary Software. Upon request, Entrust will provide Customer with a complete list of Ancillary Software and corresponding licenses, which list shall be deemed Entrust Confidential Information.

17.2. Third Party Products and Services. Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust through or in connection with the Hosted Services ("Third Party Vendor Products"). Except as expressly stated in this ECSS Schedule, Entrust has no obligation and excludes all liability with respect to Third Party Vendor Products, the use of which shall be exclusively subject to the applicable third party vendor's terms, conditions and policy documents ("Vendor Terms") accompanying, embedded in, or delivered with the Third Party Vendor Products or otherwise made available by the third party vendor. In particular:

17.2.1. If Customer purchases any Sixscape products (e.g. SixMail, SixEscrow) through Entrust or in connection with the Certificate Services, use of the Sixscape products shall be subject to the SixScape Vendor Terms embedded in or delivered with the products and those which can be retrieved at www.sixscape.com/product-and-warranty/. Entrust shall provide support in relation to the Sixscape products pursuant to the Support Schedule attached hereto.

17.2.2. If Customer uses any WebID face-to-face verification Vendor Products, use of the WebID products shall be subject to the WebID Vendor Terms that must be accepted prior to accessing such products.

Customer acknowledges and agrees that it will have the ability to submit Verification Information, including Personal Data, to WebID through the Management Account, and that WebID will deliver a data record package to Entrust to report verification results. For clarity, all processing by Entrust of Verification Information and Personal Data will be done in accordance with the Agreement, and processing by WebID will be done in accordance with the WebID Vendor Terms.

17.2.3. Entrust may make available, with certain Certificates, optional daily malware scanning services hosted by a Vendor on behalf of Entrust, as further described in the Documentation ("Malware Scanning Services"). Such Malware Scanning Services are subject to Customer supplying the information necessary to the Vendor to perform such services and accepting the Vendor Terms to receive the results. Entrust reserves the right to alter the features and functionality of the Malware Scanning Services or discontinue such services throughout the Offering Term and makes no warranty that any malware, security threats or vulnerabilities will be detected or is detectable by such services.

17.3. No Standalone Use. Any Third Party Vendor Product or Ancillary Software included with or embedded in the Offering may be used only with the applicable Offering, unless otherwise permitted in the applicable agreement accompanying such Third Party Vendor Product or Ancillary Software.

18. Reserved..

19. Publicity. During the Term and for thirty (30) days thereafter, Customer grants Entrust the right, free of charge, to use Customer's name to identify Customer as a customer on Entrust's website or other marketing or advertising materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

Exhibit A

Authorized to request a Certificate for Subscriber:	
Authorized to approve a request for a Certificate for Subscriber and to authorize others to request Certificates for Subscriber:	
Authorized to accept the subscriber agreement on Subscriber’s behalf:	

Exhibit B

Representations, Warranties, and Obligations of Subscribers and Subjects

Part 1: Subscribers

As a condition of having any Certificate issued to or for Subscriber, each Subscriber makes, on its own behalf and if applicable on behalf of its principal or agent under a subcontractor or hosting service relationship, the following representations, commitments, affirmations and warranties for the benefit of Certificate Beneficiaries, Entrust and any of Entrust's Affiliates that will issue Certificates to or for Subscriber:

For all Certificates.

1. If Subscriber is applying for a Certificate to be issued to or for another Person, such Person has authorized Subscriber to act on its behalf, including to request Certificates on behalf of such Person, and to make the representations, commitments, affirmations and warranties in this Exhibit on behalf of such Person as well as on Subscriber's own behalf.
2. All information provided, and all representations made, at all times, by Subscriber in relation to any Certificate Services, including in the Certificate request and otherwise in connection with Certificate issuance, are and will be complete, correct and accurate (and such information and representations will be promptly updated from time to time as necessary to maintain such completeness, correctness and accuracy), and does not infringe, misappropriate, dilute, unfairly compete with, or otherwise violate the intellectual property, or other rights of any person, entity, or organization in any jurisdiction. For clarity, in submitting any request for a Certificate using pre-qualified information, a Subscriber is deemed to be making anew the representations, commitments, affirmations and warranties set out in this Exhibit B, and Entrust will have no obligation to issue any Certificate containing pre-qualified information if such information is subsequently found to have changed or to be in any way inaccurate, incorrect, or misleading.
3. The private key corresponding to the public key submitted to Entrust with the Certificate request was created using sound cryptographic techniques and all reasonable measures have been taken to, at all times, assure control of (and, in the case of OV and EV code signing Certificates, sole control of), keep confidential, properly protect, and prohibit unauthorized use of, the private key (and any associated access or activation data or device, e.g., password or token), including, in the case of OV and EV code signing Certificates, in accordance with the "Data Security and Private Key Protection" provisions of the Code Signing BRs.
4. Any device storing private keys will be operated and maintained in a secure manner.
5. A Certificate will not be installed or used until Subscriber (or, in the case of code signing Certificates, Subscriber's Agent) has reviewed and verified that the content of the Certificate is accurate and correct.
6. In the case of all Entrust SSL Certificates, EV SSL Certificates and Private SSL Certificates, the Certificate will be installed only on servers that are accessible at the domain name (subjectAltName(s)) listed in the Certificate.
7. Certificates and the private key corresponding to the public key listed in such Certificate will only be used in compliance with all applicable laws and solely in accordance with the Agreement, and will only be used on behalf of the organization listed as the Subject in such Certificates.
8. The contents of Certificates will not be improperly modified.
9. Subscriber will notify Entrust, cease all use of the Certificate and the private key corresponding to the public key in the Certificate, and request the revocation of the Certificate,
   - 9.1. promptly, if any information included in the Certificate or the application for a Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
   - 9.2. immediately, if there is any actual or suspected loss, theft, misuse or compromise of the private key (or key activation data) corresponding to the public key in the Certificate, including if the value of the private key has been disclosed to an unauthorized person or an unauthorized person has had access to it ("**Key Compromise**"), or if control over the private key has been lost for other reasons.
   - 9.3. in the case of an OV or EV code signing Certificate, immediately, if there is evidence that the Certificate was used to sign Suspect Code.
10. Subscriber will promptly cease all use of the Certificate and the private key corresponding to the public key in such Certificate, upon expiration or revocation of such Certificate.
11. Subscriber will immediately respond to Entrust's instructions concerning any Key Compromise or misuse or suspected misuse of a Certificate.
12. Subscriber acknowledges and agrees that Entrust is entitled to revoke a Certificate immediately if:
    - 12.1. Customer breaches this Agreement.

12.2. Entrust discovers that there has been a Key Compromise of the Certificate's private key.
12.3. Revocation is required under the CPS or the Industry Standards.
12.4. Entrust discovers that the Certificate is compromised or being used for Suspect Code or the private key corresponding to the public key in the Certificate has been used to digitally sign Suspect Code.

13. Where the Subject named in the Certificate(s) is a separate entity from the Subscriber, the Subject has authorized the inclusion of the Subject's information in the Certificate.
14. Subscriber owns, controls, or has the exclusive right to use the domain name or email address listed in Certificate.
15. Subscriber acknowledges and agrees that Entrust is entitled to modify the Agreement when necessary to comply with any changes in Industry Standards.
16. Subscriber will use appropriate judgment about whether it is appropriate, given the level of security and trust provided by Certificate, to use the Certificate in any given circumstance.

Code Signing Certificates.

17. In addition, in the case of OV and EV code signing Certificates,

17.1. Subscriber will use commercially reasonable efforts to employ the code signing practices set out in the Code Signing Best Practices document attached hereto or by contacting Entrust ("**Code Signing Best Practices**").
17.2. Subscriber will generate and operate any device storing private keys in a secure manner, as described in the Code Signing Best Practices, and will use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport private keys.
17.3. Subscriber will not request a code signing Certificate or EV code signing Certificate containing a public key that is, or will be used with any other type of Certificate.
17.4. The Certificate and the private key corresponding to the public key in such Certificate will only be used for authorized and legal purposes, and will not be used to digitally sign Suspect Code.
17.5. An adequate network and other security controls will be provided to protect against misuse of the private key corresponding to the public key in the Certificate.
17.6. Subscriber acknowledges and agrees that Entrust is authorized to share information about the Subscriber, signed application, Certificate, and surrounding circumstances with other certification authorities or industry groups, including the CA/Browser Forum, if:

17.6.1. the Certificate or Subscriber is identified as a source of Suspect Code,
17.6.2. the authority to request the Certificate cannot be verified, or
17.6.3. the Certificate is revoked for reasons other than at Subscriber's request (e.g. as a result of private key compromise, discovery of malware, etc.).

17.7. Subscriber acknowledges that ASVs may independently determine that a Certificate is malicious or compromised and that ASVs and ASV products may have the ability to modify its customer experiences or "blacklist" an OV or EV code signing Certificate without notice to Customer or Entrust and without regard to the revocation status of the code signing Certificate.

Qualified Certificates.

18. In addition, in the case of eIDAS QWACs, PSD2 QWACs, eIDAS QSealCs, PSD2 QSealCs, and eIDAS QSigCs,

18.1. Subscriber will comply with any requirements in the CPS for it to use a specific type of cryptographic device (including a secure cryptographic device or a qualified electronic signature/seal creation device "QSCD"), and if so required:

18.1.1. the Subject's private key(s) will only be used for cryptographic functions within the specified cryptographic device.
18.1.2. if the Subject's keys are generated under control of the Subscriber or Subject, the Subject's keys will be generated within the specified cryptographic device.

18.2. Subscriber consents to Entrust's keeping of a record of information used in registration, subject device provision, including whether this is to the Subscriber or to the Subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required by Industry Standards in the case of Entrust terminating its services.
18.3. Subscriber requires the publication of the Certificate in the manner and in accordance with the conditions set out in the CPS and will obtain, where applicable, the Subject's consent to such publication.
18.4. The private key and corresponding public key associated with the Certificate will only be used in accordance with the limitations notified to the Subscriber, including in the CPS.

18.5. If the Subscriber or Subject generates the Subject's keys:
   18.5.1. the Subject keys will be generated using an algorithm as specified in the Industry Standards for the uses of the certified key as identified in the CPS.
   18.5.2. the key length and algorithm will be as specified in the Industry Standards for the uses of the certified key as identified in the CPS during the validity time of the Certificate.
   18.5.3. the Subject's Private Key will be maintained under the Subject's control, and, if the Subject is an individual, the Subject's sole control.

18.6. The Subject's private key will be used under the Subject's control, and, if the Subject is an individual, the Subject's sole control.

18.7. Upon being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, Subscriber will ensure that the private key corresponding to the public key in the Certificate is no longer used by the Subject.

18.8. In respect to eIDAS QSigC, key pairs will only be used for electronic signatures.

18.9. In respect to eIDAS QSealC and PSD2 QSealC, key pairs will only be used for electronic seals.

Verified Mark Certificates.

19. In addition, in the case of VMCs:
   19.1. Subscriber will apply for and use VMCs in accordance with and subject to the VMC Requirements.
   19.2. The trademarks submitted in a VMC application represent registered trademarks that the Subscriber owns or for which it has obtained sufficient license to be able to grant the limited license in the Terms of Use attached to the VMC Requirements, and that it will immediately revoke the VMC if it no longer owns or has a sufficient license to the applicable trademarks.

Part 2: Individual Subjects, when different from the Subscriber

If the Subject and Subscriber are separate entities and the Subject is a Person (i.e. not a device), as a condition of having any eIDAS QWAC, PSD2 QWAC, eIDAS QSealC, PSD2 QSealC and eIDAS QSigC issued to or for it, the Subject accepts the following obligations:

1. Subject will comply with any requirements in the CPS for it to use a specific type of cryptographic device (including a secure cryptographic device or QSCD), and if so required, the Subject's private key(s) will only be used for cryptographic functions with the specified cryptographic device.
2. Subject consents to Entrust's keeping of a record of information used in registration, subject device provision, including whether this is to the Subscriber or to the Subject where they differ, and any subsequent revocation, the identity and any specific attributes placed in the Certificate, and the passing of this information to third parties under the same conditions as required by ETSI EN 319 411-1 in the case of Entrust terminating its services.
3. Private key and corresponding public key associated with the Certificate will only be used in accordance with the limitations notified to the Subject, including in the CPS.
4. Subject will prohibit unauthorized use of the Subject's private key.
5. If the Subject generates the Subject's keys, the Subject's private key will be maintained under the Subject's control, and, if the Subject is an individual, the Subject's sole control.
6. The Subject's private key will be used under the Subject's control, and, if the Subject is an individual, the Subject's sole control.
7. Subject will notify Entrust immediately:
   7.1. if any information included in the Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate misleading.
   7.2. and immediately and permanently discontinue use of the applicable key, if there is any actual or suspected loss, theft, misuse or compromise of the private key (or key activation data) corresponding to the public key in the Certificate, including if the value of the private key has been disclosed to an unauthorized person or an unauthorized person has had access to it, or if control over the private key has been lost for other reasons.
8. Upon being informed that the Subject's Certificate has been revoked, or that the issuing CA has been compromised, Subject will no longer use the private key.

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope**.

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery.** Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty.**

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination.**

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users.** Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source**. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms")**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. "**Business Day**" means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. "**Covered Offering**" means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. "**Customer-Hosted Offering**" means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer's premises.

1.4. "**Extended Support**" means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. "**Hosted Service**" for the purposes of this Schedule means Entrust's Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. "**Incident**" means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. "**Named Support Contacts**" means individual Users nominated by Customer to act as Customer's support representatives.

1.8. "**Problem**" means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. "**Production Environment**" means Customer's live business environment with active users.

1.10. "**Response Time**" means the amount of time that elapses between the Customer's report of a Service Request to Entrust and Entrust's acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. "**Service Plan**" means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**" means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. "**Software**" for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. "**Superseded Product**" means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain

additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees.**

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer's Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail ("Immediate Incident Response Time").

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. <u>Upgrades for Customer-Hosted Offerings</u>.

8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. "for Windows") and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. "for Mac"), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions**.

9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer's failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer's use of the Covered Offering shall be at Customer's own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a "no charge", beta testing, proof of concept, evaluation or "not for resale" basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act).

Code Signing Best Practices

Code Signing Best Practices

The biggest issue with code signing is the protection of the private signing key associated with the code signing certificate. If a key is compromised, the certificate loses trust and value, jeopardizing the software that you have already signed.

Consider the following code signing best practices:

1. Minimize access to private keys
    - Allow minimal connections to computers with keys
    - Minimize the number of users who have key access
    - Use physical security controls to reduce access to keys

2. Protect private keys with cryptographic hardware products
    - Cryptographic hardware does not allow export of the private key to software where it could be attacked
    - Use a FIPS 140 Level 2-certified product (or better)
    - If private keys will be transported, ensure the cryptographic hardware is protected with a randomly generated password of at least 16 characters which contains uppercase letters, lowercase letters, numbers and special characters

3. Time-stamp code
    - Time-stamping allows code to be verified after the certificate has expired or been revoked
    - Time-stamp certificates can be issued for a maximum of 135 months which can support the signed software to be validated for up to 11 years

4. Understand the difference between test-signing and release-signing
    - Test-signing private keys and certificates requires less security access controls than production code signing private keys and certificates
    - Test-signing certificates can be self-signed or come from an internal test CA
    - Test certificates must chain to a completely different root certificate than the root certificate that is used to sign publicly released products; this precaution helps ensure that test certificates are trusted only within the intended test environment
    - Establish a separate test code signing infrastructure to test-sign pre-release builds of software

5. Authenticate code to be signed
    - Any code that is submitted for signing should be strongly authenticated before it is signed and released
    - Implement a code signing submission and approval process to prevent the signing of unapproved or malicious code
    - Log all code signing activities for auditing and/or incident-response purposes

6. Virus scan code before signing
    - Code signing does not confirm the safety or quality of the code; it confirms the publisher and whether or not the code has been changed
    - Take care when incorporating code from other sources
    - Implement virus-scanning to help improve the quality of the released code

7. Do not over-use any one key (distribute risk with multiple certificates)
    - If code is found with a security flaw, then publishers may want to prompt a User Account Control dialogue box to appear when the code is installed in the future; this can be done by revoking the code signing certificate so a revoked prompt will occur
    - If the code with the security flaw was issued before more good code was issued, then revoking the certificate will impact the good code as well
    - Changing keys and certificates often will help to avoid this conflict

8. Revoking compromised certificates
    - Report key compromise or signed malware to your certification authority
    - Compromised keys or signed malware of suspect code will require the code signing certificate to be revoked
    - Assuming that all signed code has been time-stamped, then the revocation date can be selected before the time of compromise. This will mean that code signed before the revocation date may not be impacted.

References

The following references will support Windows and Java code signing.

- Guide to Code Signing for Authenticode
- Guide to Code Signing for Java
- Guide to Code Signing for Windows Macros & Visual Basic
- Guide to Code Signing and EV Code Signing Certificate for Download and Installation

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope.**

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery**. Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty**.

   6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

   6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

   6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination**.

   7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

   7.2. Termination. In addition to the termination rights in the General Terms:

      7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract

Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users.** Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source.** Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms")**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. “**Business Day**” means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. “**Covered Offering**” means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. “**Customer-Hosted Offering**” means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer’s premises.

1.4. “**Extended Support**” means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. “**Hosted Service**” for the purposes of this Schedule means Entrust’s Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. “**Incident**” means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. “**Named Support Contacts**” means individual Users nominated by Customer to act as Customer’s support representatives.

1.8. "**Problem**” means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. “**Production Environment**” means Customer’s live business environment with active users.

1.10. “**Response Time**” means the amount of time that elapses between the Customer’s report of a Service Request to Entrust and Entrust’s acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. “**Service Plan**” means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**” means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. “**Software**” for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. “**Superseded Product**” means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. “**Support Services**” means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. “**Upgrade**” in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **<u>Support Provision</u>.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **<u>Additional Benefits.</u>** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **<u>Support Term</u>.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **<u>Support Fees</u>.**

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer's Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail ("Immediate Incident Response Time").

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. **Upgrades for Customer-Hosted Offerings**.

8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. "for Windows") and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. "for Mac"), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions**.

9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer's failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer's use of the Covered Offering shall be at Customer's own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a "no charge", beta testing, proof of concept, evaluation or "not for resale" basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of

the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act).

General Terms and Conditions

This Agreement (as defined below) is made as of the date set forth in the Order ("Effective Date") between the Ordering Activity under the GSA Schedule contract identified in the Order ("Customer") and Entrust Corporation ("Entrust").

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Contract Structure and Parties.**

   1.1. These General Terms govern access to and use of any one or more of the following Entrust products and services (each, an "Offering"): (a) one or more executable software modules and associated deployment tools in machine-readable form ("Software"); (b) managed or cloud services hosted by Entrust or its hosting providers ("Hosted Service"); (c) technical support, training and Software maintenance ("Support"); and (d) consulting and other professional services ("Professional Services"). Each Offering consists of the features, and is further subject to the offering-specific terms and conditions, set out in the applicable terms of use or schedule attached hereto, or available at https://www.entrust.com/legal-compliance/terms-conditions (each set of terms of use and each schedule, a "Schedule").

   1.2. An "Order" for one or more Offering(s) means (i) a Customer-issued purchase order (excluding any terms and conditions thereon) that refers to a valid Entrust quote for one or more Offering(s) and incorporates these General Terms; (ii) an electronic order submitted via Entrust's online portal which facilitates transactions over the Internet; (iii) an order acknowledgement issued by Entrust and signed by or on behalf of Customer; or (iv) a statement of work for Professional Services (defined below) duly signed by each party.

   1.3. Each Order, together with these General Terms and the applicable Schedule(s) for the Offering(s) listed on the Order constitute the "Agreement" between Customer and Entrust. In the Agreement, "Affiliate" means, with respect to Entrust, any subsidiary of Entrust Corporation, and, with respect to Customer, any corporation or other entity that is directly or indirectly controlled by Customer either through ownership of fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control.

2. **Customer's Users.** Customer is responsible for the use of the Offering by any individual, organization or legal entity (each, a "Person") who directly or indirectly receives access to, or the ability to use, the Offering or any component thereof through the Customer, including any such Persons more specifically described in the user guide, manual, technical specifications or release notes for the applicable Offering provided by Entrust, all as may be updated from time to time ("Documentation") or described in the applicable Schedule (each such Person, a "User"). Any act or omission of a User with respect to an Offering is deemed to be the act or omission of Customer.

3. **Software.** If an Order calls for any Software to be provided to Customer (whether or not as part of or in connection with another Offering), the Schedule provided with the Software will apply. If no more specific Schedule is provided with the Software, the Schedule for the Software is the end user license available at https://www.entrust.com/-/media/documentation/licensingandagreements/certificate-solutions-software-schedule.pdf.

4. **Hosted Services**. If an Order calls for any Hosted Services to be provided to Customer (whether or not as part of or in connection with another Offering), the Schedule provided with the Hosted Service will apply.

5. **Support.** If an Order calls for Support to be provided by Entrust for an Offering, any such support will be provided pursuant to the then-current Support Schedule for the applicable Offering as referenced within the applicable Offering Schedule or available at https://www.entrust.com/legal-compliance/terms-conditions. Where support is purchased through an authorized reseller and the Order indicates that the reseller will provide support, then such support will be provided by the authorized reseller (and not Entrust).

6. **Professional Services.** If Entrust provides any Professional Services and deliverables with respect to any Offering, these General Terms will include the additional terms in the Professional Services Schedule attached hereto with respect to such Professional Services. An additional Schedule and/or an Order will further set out the scope and details of any Professional Services, including, if and as applicable, resource specialist(s), milestones, delivery dates, acceptance criteria, payment terms and any other information and terms related to the Professional Services.

7. **Other Entrust Products**. Certain Entrust hardware, equipment and supplies, including any associated firmware ("Hardware"), and other Entrust products or services that are not Offerings as defined herein (collectively, "Additional Entrust Products and Services") may be sold, distributed, provided or otherwise made available to Customer (whether or not as part of or in connection with an Offering). Such Additional Entrust Products and Services will be subject to the applicable separate Entrust agreements that accompany such Additional Entrust Products and Services or that are otherwise made available by Entrust.

8. **General Restrictions**. Customer will not: (a) host, time-share, rent, lease, sell, license, sublicense, assign, distribute or otherwise transfer or allow third parties to exploit any component of any Offering, except as provided in the Agreement; (b) copy, modify, translate, reverse engineer, de-compile or disassemble, or create derivative works from any Offering except to the extent that law explicitly prohibits this restriction notwithstanding a contractual restriction to the contrary; (c) attempt to circumvent or disable any restriction or entitlement mechanism that is present or embedded in any component provided as part of any Offering, including the Data Protection representations and warranties set out in Section 12; (d) provide any passwords or other log-in information provided by Entrust as part of any Offering to any third party; (e) share non-public features or content of any Offering with any third party; (f) access any Offering in order to build or benchmark against a competitive product or service, or to build a product or service using similar ideas, features, or functions of any Offering; (g) use any Offering to send or store infringing or unlawful material or viruses, worms, time bombs, Trojan horses and other harmful or malicious codes, files, scripts, agents or programs; (h) use any Offering bundled with or provided for use with another Offering independently of the applicable bundle or Offering with which it is intended to be used; (i) use any Offering other than in compliance with all applicable laws and regulations; (j) misuse or misconfiguration of any Offering; or (k) use any Offering other than in compliance with the Agreement.

9. **Fees and Taxes**. Customer will pay to Entrust or its authorized reseller, as applicable, the amounts set forth in the Order(s) (including where overages are applicable, any overage fees) in accordance with the GSA Schedule Pricelist. All amounts due under the Agreement to Entrust must be paid to the Entrust Affiliate or its authorized reseller that issued the applicable invoice. Except as otherwise stated in the applicable Order, fees will be invoiced at the beginning of the Offering Term, and Customer will pay all amounts payable under the Agreement within thirty (30) days of the date of the invoice receipt, without setoff or counterclaim, and without any deduction or withholding. Entrust shall state separately on its invoices taxes excluded from the fees, and the Customer agrees either to pay the amount of the taxes (based on the current value of the Offering) or provide evidence necessary to sustain an exemption, in accordance with 552.212-4(k). Entrust may elect to charge Customer interest for late fees at the interest rate established by the Secretary of the Treasury as provided in 41.U.S.C. 7109, which is applicable to the period in which the amount becomes due, and then at the rate applicable for each six-month period as fixed by the Secretary until the amount is paid. Notwithstanding any of the foregoing, if Customer has purchased through an Entrust authorized reseller then the terms relating to fees and taxes will be those terms established between Customer and such reseller instead of those set out above.

10. **Term and Termination**.

10.1. The General Terms and Schedules shall be in effect commencing on the date the first Order is accepted and will remain effective for a period of three (3) years and may be renewed for successive one-year periods thereafter by executing a written Order for the renewal term.

10.2. The obligations with respect to each Offering will commence on the date that the Order for the Offering is accepted by Entrust, unless otherwise specified in the Order or in the applicable Offering Schedule, and will remain effective for the period specified in the Order or in the applicable Offering Schedule, unless terminated earlier in accordance with this Agreement ("Offering Term").

10.3. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

10.4. Effects of Termination and Expiration

10.4.1. Termination or Expiration of General Terms. Termination or expiration (non-renewal) of the General Terms also terminates all Schedules and the parties' ability to enter into any new Orders (including Orders to renew). If there are any ongoing Offerings as at the date of a termination notice, the termination notice must specify whether it terminates the Agreement with respect to such Offering(s). If there are any ongoing Offerings as at the date of a non-renewal notice, unless the non-renewal notice also expressly provides a notice of termination pursuant to the Agreement with respect to the ongoing Offering, the Order for the ongoing Offering will remain effective until the end of the then-current Offering Term, and the General Terms and Schedules will survive in respect of that Offering and continue to govern such Offering until the end of the current Offering Term. During such survival period, no new Orders (including any Orders to renew) may be made.

10.4.2. Termination of Agreement for Offerings. Upon termination of the Agreement for any Offering, Entrust will have no further obligation to provide the Offering, Customer will immediately cease all use of the Offering, and Customer will destroy any copies of documentation and delete any software Offering in its possession or control.

10.4.3. General. Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Any provision of this Agreement which contemplates or requires performance after the termination of this Agreement or that must survive to fulfill its essential purpose, including the terms of this Section (Term and Termination), confidentiality, disclaimers, limitations and exclusions of liability, and any payment obligations, will survive the termination and continue in full force and effect until completely performed.

10.4.4. Termination Fees. In the event of any termination by Customer for Offerings Entrust provided prior to the termination date, Customer is required to pay to Entrust any unpaid fees for any terminated Offerings in accordance with Section 9 (Fees and Taxes).

11. **<u>Confidentiality</u>.** In this Section (Confidentiality), “Discloser” means the party that discloses Confidential Information (defined below), and “Recipient” means the party that receives it. If Confidential Information is disclosed or received by an Affiliate of a party, it is deemed to have been disclosed or received by the party itself. The Recipient will use all Confidential Information it receives only for the purpose of exercising its rights and fulfilling its obligations under the Agreement. Recipient will treat such Confidential Information with the same degree of care against unauthorized use or disclosure that it affords to its own information of a similar nature, but no less than reasonable degree of care. Recipient will not remove or destroy any proprietary or confidential legends or markings placed upon any documents or other materials. Recipient will only disclose Discloser’s Confidential Information to Recipient’s and its Affiliates’ personnel and agents with a need to know (“Recipient Agents”). Recipient shall be responsible for ensuring Recipient Agents comply with the confidentiality obligations of this Section (Confidentiality) and any acts or omissions of a Recipient Agent in breach of the terms and conditions of this Section (Confidentiality) shall be considered the acts or omissions of the Recipient. “Confidential Information” means any business, technical, financial, or other information, however conveyed or presented to the Recipient, that is clearly designated by the Discloser as being confidential or that ought reasonably to be considered confidential by the Recipient, including all information derived by the Recipient from any such information. Confidential Information does not include any information that: (i) is expressly excluded from the definition of Confidential Information in an applicable Schedule; (ii) was lawfully known by Recipient prior to disclosure; (iii) was lawfully in the public domain prior to its disclosure, or becomes publicly available other than through a breach of the Agreement; (iv) was disclosed to Recipient by a third party without a duty of confidentiality to the Discloser; or (v) is independently developed by Recipient without reference to Discloser’s Confidential Information. If Recipient is compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law, to disclose Confidential Information of the Discloser, Recipient will use reasonable efforts to seek confidential treatment for such Confidential Information, and, if and as permitted by law, will provide prior notice to the Discloser to allow the Discloser to seek protective or other court orders. Entrust recognizes that Federal agencies are subject to the Freedom of Information Act, 5 U.S.C. 552, which may require that certain information be released, despite being characterized as “confidential” by Entrust. Personal Data and Excluded Data (each as defined in Section 12 (Data Protection) below) are excluded from the general definition of “Confidential Information” and the application of this Section (Confidentiality) but are subject to the specific confidentiality and other provisions of Section 12 (Data Protection).

12. **<u>Data Protection</u>**.

12.1. To the extent that Entrust processes any Personal Data (as defined in the latest version of Entrust’s customer data processing agreement (“DPA”), which is attached hereto on Customer’s behalf and in performance of the Agreement, the terms of the DPA, which are attached hereto and hereby incorporated by reference, shall apply and the parties agree to comply with such terms. Customer's acceptance of this Agreement shall be treated as acceptance and signing of the DPA (including the Standard Contractual Clauses attached to the DPA). Entrust reserves the right to non-materially update the DPA from time to time to comply with legal and regulatory requirements, and to keep current with upgrades and enhancements to its products and services. Entrust will provide notice in the event of any such updates. The latest version posted on Entrust's website shall always apply.

12.2. Customer represents and warrants that it will not provide or transfer or cause to be provided or transferred to Entrust any Excluded Data, except if and as the provision or transfer of Excluded Data is expressly required and addressed in a Schedule. "Excluded Data" means: (i) social security numbers or their equivalent (e.g., social insurance numbers), driver license numbers, and health card numbers; (ii) other personal data that would be considered sensitive in nature including information regarding racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation; (iii) data falling into a "special category of data" under EU General Data Protection Regulation; (iv) "cardholder data" as defined by the Payment Card Industry Data Security Standards; (v) data regulated under the Health Insurance Portability and Accountability Act or the Gramm-Leach-Bliley Act or similar laws or regulations in place now or in the future in the applicable jurisdiction (collectively, the "Excluded Data Laws"). Customer recognizes and agrees that, except to the extent specified in a Schedule: (i) Entrust has no liability for any failure to provide protections set forth in the Excluded Data Laws or otherwise to protect excluded data; and (ii) Entrust's Offerings are not intended for management or protection of Excluded Data and may not provide adequate or legally required security for Excluded Data.

13. **Disclaimer of Warranties**.

Any warranties for Offerings will be expressly stated in the applicable Schedule or Order; except as may be so expressly stated in the applicable Schedule or Order, each Offering is provided "as is", and Entrust and its Affiliates, licensors and suppliers disclaim any and all representations, conditions or warranties of any kind, express or implied, including warranties of non-infringement, title, merchantability or fitness for a purpose, satisfactory quality, or any representations, conditions or warranties implied by statute, course of dealing, course of performance, or usage or trade. Entrust makes no representations, conditions or warranties regarding any third party product or service, including any Third Party Vendor Product as defined below, with which any Offering may interoperate. Entrust makes no representations, conditions or warranties that any Software will perform without interruption or error. If a warranty for the Offering is not expressly stated in the applicable Schedule or Order, then Entrust warrants that the Offering will, for a period of sixty (60) days from the date of delivery, perform substantially in accordance with the Offering's Documentation. This warranty shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) Customer's failure to use the Offering in accordance with the Agreement and the Documentation; (ii) Customer's misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Offering; or (iii) any modifications or additions made to the Offering by Customer or by a third party acting for the Customer. Entrust's exclusive liability and the Customer's sole and exclusive remedy for Entrust's breach of the provisions of this warranty shall be, at Entrust's option, to correct, repair or replace, free of charge, the Offering which does not meet Entrust's warranty.

14. **Indemnities**.

14.1. **Intellectual Property Claims.**

14.1.1. Intellectual Property Indemnity. Entrust shall have the right to intervene to defend at its expense (including, for clarity, bearing court costs and reasonable attorney's fees) Customer against any claims by third parties that the Software and/or Hosted Service furnished and used within the scope of the Agreement infringes upon or misappropriates a patent, trademark, copyright, trade secret or other intellectual or proprietary right (an "IP Claim"), and will pay any (i) amounts finally awarded against Customer by a court or arbitrator in any proceeding related to such IP Claim or (ii) settlement amounts approved in accordance with this Section (Indemnities). Nothing contained herein shall be construed in derogation of the U.S. Department of Justice's right to defend any claim or action brought against the U.S., pursuant to its jurisdictional statute 28 U.S.C. §516.

14.1.2. **Mitigation by Entrust. If (i) Entrust becomes aware of an actual or potential IP Claim, or (ii) Customer provides Entrust with notice of an actual or potential IP Claim, Entrust may (or in the case of an injunction against Customer, shall), at Entrust's sole option and expense: (i) procure for Customer the right to continue to use the affected portion of the Software or Hosted Service; (ii) modify or replace the affected portion of the Software or Hosted Service with functionally equivalent or superior software so that Customer's use is non-infringing; or (iii) if (i) or (ii) are not commercially reasonable, terminate the Agreement with respect to the affected Software or Hosted Service and refund to the Customer, as applicable, either (A) any perpetual license fees paid for the affected Software depreciated over a three (3) year period from the date of delivery on a straight line basis less any outstanding moneys owed on such affected portion of the Software; or (B) any prepaid and unused subscription fees for the affected Software or Hosted Service for the terminated portion of the applicable Offering Term.**

14.1.3. **Exceptions to Indemnity. Entrust shall have no liability for any IP Claim in respect of any Software or Hosted Service to the extent that: (i) such Software or Hosted Service is used by Customer outside the scope of the rights granted in the Agreement or in a manner or for a purpose other than that for which it was supplied, as contemplated by the Documentation; (ii) such Software or Hosted Service is modified by Customer; (iii) such Software or Hosted Service is used by Customer in combination with other software or services not provided by Entrust and the infringement arises from such combination or the use thereof; (iv) the IP Claim arises from information, data or specifications provided by Customer; (v) the Software or Hosted Service was provided on a beta testing, proof of concept, evaluation or "not for resale" basis; or (vi) the IP Claim relates to the use of any version of the Software other than the current, unaltered release, if such IP Claim would have been avoided by the use of a current unaltered release of the Software.**

14.1.4. **THE PROVISIONS OF THIS SECTION 14 (INTELLECTUAL PROPERTY CLAIMS) ARE SUBJECT TO SECTION 15 (LIABILITY) AND STATE THE SOLE AND EXCLUSIVE LIABILITY OF ENTRUST AND ITS AFFILIATES AND THE SOLE AND EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO ANY CLAIM OF THE NATURE HEREIN.**

14.2. **Reserved.**

14.3. **Conditions. The obligations in this Section (Indemnities) will apply only if indemnified party: (i) provides the indemnifying party prompt written notice of the IP Claim or Customer Indemnified Claim ("Claim"), provided that failure by the indemnified party to provide prompt notice will relieve the indemnifying party of its obligations only to the extent that the indemnifying party was actually and materially prejudiced by such failure; (ii) gives the indemnifying party the exclusive right to control and direct the investigation and defense of such Claim, including appeals, negotiations, and any settlement or compromise thereof, provided that the indemnified party will have the right to reject any settlement or compromise that requires that it or they admit wrongdoing or liability or that subjects it or them to any ongoing affirmative obligations; (iii) has not compromised or settled the Claim; and (iv) agrees to cooperate and provide reasonable assistance (at indemnifying party's sole expense) in the defense.**

15. **Liability.**

15.1. **In this Section (Liability), "Entrust" will be deemed to mean Entrust Corporation, its Affiliates, and their respective suppliers, licensors, resellers, distributors, subcontractors, directors, officers, and personnel.**

15.2. **In no event will Entrust be liable for, and Customer waives any right it may have to, any consequential, indirect, special, incidental, punitive or exemplary damages or for any loss of business, opportunities, revenues, profits, savings, goodwill, reputation, customers, use, or data, or costs of reprocurement or business interruption. For any given Offering, in no event will Entrust's total aggregate liability arising out of or related to the Agreement or the use and performance of the Offering exceed the fees paid to Entrust for the Offering for the twelve months prior to the first event giving rise to liability, less any refunds, service credits or deductions.**

15.3. **The exclusions and limits in this Section (Liability) apply: (a) regardless of the form of action, whether in contract (including fundamental breach), tort (including negligence),**

warranty, indemnity, breach of statutory duty, misrepresentation, strict liability, strict product liability, or otherwise; (b) on an aggregate basis, regardless of the number of claims, transactions, digital signatures or certificates; (c) even if the possibility of the damages in question was known or communicated in advance and even if such damages were foreseeable; and (d) even if the remedies fail of their essential purpose. Customer acknowledges that Entrust has set its prices and entered into the Agreement in reliance on the limitations and exclusions in this Section (Liability), which form an essential basis of the Agreement.

15.4. **Notwithstanding anything to the contrary in this Section (Liability) or elsewhere in the Agreement, to the extent required by applicable law Entrust neither excludes nor limits its liability for: (i) death or bodily injury caused by its own negligence; (ii) its own fraud or fraudulent misrepresentation; or (iii) other matters for which liability cannot be excluded or limited under applicable law.**

16. **Nature of Relationship**. Nothing contained in the Agreement will be deemed to constitute either party or any of its employees, the partner, agent, franchisee, or legal representative of the other party or to create any fiduciary relationship for any purpose whatsoever. Except as otherwise specifically provided in the Agreement, nothing in the Agreement will confer on either party or any of its employees any authority to act for, bind, or create or assume any obligation or responsibility on behalf of the other party. The parties agree that no Entrust personnel is or will be considered the personnel of Customer.

17. **Subcontractors.** Entrust may use one or more Affiliate(s) or subcontractors to perform its obligations under the Agreement, provided that such use will not affect Entrust's obligations under the Agreement.

18. **Third Party Products and Services**.

18.1. Third Party Vendor Products. Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust ("Third Party Vendor Products"). Third Party Vendor Products are subject to the applicable third party's agreement that accompanies such Third Party Vendor Product or that is otherwise made available by such third party.

18.2. Ancillary Software. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Offering ("Ancillary Software"). If a separate license agreement pertaining to Ancillary Software is embedded or provided with the Offerings, then the Ancillary Software is subject to the applicable separate license agreement pertaining to the Ancillary Software. Upon request, Entrust will provide Customer with a complete list of Ancillary Software and corresponding licenses, which list shall be deemed Entrust Confidential Information.

18.3. No Standalone Use. Any Third Party Vendor Product or Ancillary Software included with or embedded in the Offering may be used only with the applicable Offering, unless otherwise permitted in the applicable agreement accompanying such Third Party Vendor Product or Ancillary Software.

19. **Reserved**.

20. **High Risk Applications.** Customer may not use, or authorize others to use, any part of any Offering in any application in which the failure of the Offering could lead to death, personal injury or severe physical or property damage ("High-Risk Applications"), including the monitoring, operation or control of nuclear facilities, mass transit systems, aircraft navigation or aircraft communication systems, air traffic control, weapon systems and direct life support machines. Entrust expressly disclaims any express or implied warranty of fitness for High Risk Applications.

21. **No Exclusivity**. Nothing in the Agreement shall prevent Entrust or its Affiliates from providing to a third party the same or similar products, services or deliverables as those provided to the Customer pursuant to the Agreement.

22. **Notices**. In any case where any notice or other communication is required or permitted to be given, such notice or communication will be in writing and (a) personally delivered, in which case it is deemed given and received upon receipt or (b) sent by international air courier service with confirmation of delivery to the addresses stated below, in which case it is deemed given and received when delivery is confirmed.

Notices to Customer: the address stipulated in the Order.

Notices to Entrust: 1187 Park Pl., Shakopee, MN 55379-3817, USA

23. **<u>Choice of Law</u>**. Any disputes related to the products and services offered under the Agreement, as well as the construction, validity, interpretation, enforceability and performance of the Agreement, shall be governed by the Federal laws of the United States. In the event that any matter is brought in a provincial, state or federal court each party waives any right that such party may have to a jury trial. To the maximum extent permitted by applicable law, the parties agree that the provisions of the United Nations Convention on Contracts for the International Sale of Goods, as amended, shall not apply to the Agreement. This Section (Choice of Law) governs all claims arising out of or related to this Agreement, including tort claims.

24. **<u>Force Majeure</u>**. Excusable delays shall be governed by GSA Schedule Contract Clause 552.212-4(f).

25. **<u>No Waiver</u>**. No failure to exercise, no delay in exercising, and no statement or representation other than by any authorized representative in an explicit written waiver, of any right, remedy, or power will operate as a waiver thereof, nor will single or partial exercise of any right, remedy, or power under the Agreement preclude any other or further exercise thereof or the exercise of any other right, remedy, or power provided in the Agreement, in law, or in equity. The waiver of the time for performance of any act or condition under the Agreement does not constitute a waiver of the act or condition itself.

26. **<u>Successors; Assignment</u>**. Each party agrees that it will not (and neither party has any right to) assign, sell, transfer, or otherwise dispose of, whether voluntarily, involuntarily, by operation of law, or otherwise, the Agreement or any right or obligation under the Agreement without the prior written consent of the other party. Any purported assignment, sale, transfer, delegation or other disposition in violation of this Section (Successors; Assignment) will be null and void. Notwithstanding the foregoing, Entrust may, assign the Agreement together with all of its rights and obligations under the Agreement (i) to an Affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets of the business to which the Agreement relates in accordance with the provisions set forth at FAR 42.1204. Subject to the foregoing limits on assignment and delegation, the Agreement will be binding upon and will inure to the benefit of the Parties and their respective successors and permitted assigns.

27. **<u>Compliance with Applicable Laws</u>**. Customer will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection with Customer's exercise of its rights and obligations under any part of the Agreement, including use or access by Users. Without limiting the foregoing, Customer will comply with all applicable trade control laws, including but not limited to any sanctions or trade controls of the European Union ("E.U."), Canada, the United Kingdom ("U.K."), and United Nations ("U.N."); the Export Administration Regulations administered by the United States ("U.S.") Department of Commerce's Bureau of Industry and Security; U.S. sanctions regulations administered by the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"); or on the U.S. Department of Commerce Entities List ("Entities List"); and any import or export licenses required pursuant to any of the foregoing; and all applicable anti-money laundering laws, including the U.S. Bank Secrecy Act, Money Laundering Control Act, and Patriot Act, the Canadian Proceeds of Crime (Money Laundering) and Terrorist Financing Act, the U.K. Proceeds of Crime Act, and legislation implementing the International Convention on the Suppression of the Financing of Terrorism or the money laundering provisions of the U.N. transnational Organized Crime Convention. Customer represents and warrants that: (a) neither Customer nor any User is located in, under the control of, or a national or resident of any country to which the export of any software or technology licensed under the Agreement, or related information, would be prohibited by the applicable laws, rules or regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (b) neither Customer nor any User is a Person to whom the export of any software or technology licensed under the Agreement, or related information, would be prohibited by the laws of the U.S., Canada, U.K., E.U., or other applicable jurisdiction; (c) Customer and each User has and will comply with applicable laws, rules and regulations of the U.S., Canada, U.K., E.U., or other applicable jurisdiction(s) and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust; (d) Customer and all Users will not use any Offering for any purposes prohibited by applicable laws, rules or regulations on trade controls, including related to nuclear, chemical, or biological weapons proliferation, arms trading, or in furtherance of terrorist financing; (e) neither Customer nor any User nor any of its affiliates, officers, directors, or employees is (i) an individual listed on, or directly or indirectly owned or controlled by, a Person (whether legal or natural) listed on, or acting on behalf of a Person listed on, any U.S, Canadian, E.U., U.K., or U.N. sanctions list, including OFAC's list of Specially Designated Nationals or the Entities List; or (ii) located in, incorporated under the laws of, or owned (meaning 50% or greater ownership interest) or otherwise, directly or indirectly, controlled by, or acting on behalf of, a person located in, residing in, or organized under the laws of any of the countries listed at https://www.entrust.com/legal-compliance/denied-parties (each of (i) and (ii), a

"Denied Party"); and (f) Customer and each of its Users is legally distinct from, and not an agent of any Denied Party. In the event any of the above representations and warranties is incorrect or the Customer or any User engages in any conduct that is contrary to sanctions or trade controls or other applicable laws, regulations, or rules, any Agreements, purchase orders, performance of services, or other contractual obligations of Entrust are immediately terminated.

28. **No Other Rights Granted**. The rights granted under the Agreement are only as expressly set forth in the Agreement. No other right or interest is or will be deemed to be granted, whether by implication, estoppel, inference or otherwise, by or as a result of the Agreement or any conduct of either party under the Agreement. Entrust and its licensors expressly retain all ownership rights, title, and interest in the products and services provided by Entrust (including any modifications, enhancements and derivative works thereof). Any permitted copy of all or part of any item provided to Customer must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust to Customer.

29. **Order of Precedence**. A provision in an Order executed by both parties will prevail over any conflicting provision elsewhere in the Agreement, and, subject to the foregoing, a provision in a Schedule will prevail with respect to the applicable Offering over any conflicting provision in the Agreement.

30. **Entire Agreement**. The Agreement (as defined in Section 1 (Contract Structure and Parties)) and items expressly incorporated into any part of the Agreement form the entire agreement of the parties. All terms and conditions on any purchase orders, supplier registration forms, supplier code of conduct, or similar document issued by Customer shall not amend the terms of the Agreement and will be of no force or effect notwithstanding any term or statement to the contrary made in such document. Neither party has entered into the Agreement in reliance upon any representation, warranty, condition or undertaking of the other party that is not set out or referred to in the Agreement.

31. **Amendment**. The Agreement may not be modified except by formal agreement in writing executed by both parties.

32. **Severability**. To the extent permitted by applicable law, the parties hereby waive any provision of law that would render any provision of the Agreement invalid or otherwise unenforceable in any respect. In the event that a provision of the Agreement is held to be invalid or otherwise unenforceable in application to particular facts or circumstances: (a) such provision will be interpreted and amended to the extent necessary to fulfill its intended purpose to the maximum extent permitted by applicable law and its validity and enforceability as applied to any other facts or circumstances will not be affected or impaired; and (b) the remaining provisions of the Agreement will continue in full force and effect. For greater certainty, it is expressly understood and intended that each provision that deals with limitations and exclusions of liability, disclaimers of representations, warranties and conditions, or indemnification is severable from any other provisions.

33. **Language.** The definitive version of this Agreement is written in English. If this Agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls. If Customer is located in Quebec, the parties hereby confirm that they have requested that this Agreement and all related documents be drafted in English; les parties ont exigé que le présent contrat et tous les documents connexes soient rédigés en anglais. Some versions of the Offerings which have been designated as localized or country-specific may nonetheless contain certain components and/or interfaces that are in the English language only.

34. **Interpretation**. The parties agree that the Agreement will be fairly interpreted in accordance with its terms without any strict construction in favor of or against either party, and that ambiguities will not be interpreted against the party that drafted the relevant language. In the Agreement, the words "including", "include" and "includes" will each be deemed to be followed by the phrase "without limitation". The section or other headings in the Agreement are inserted only for convenience and ease of reference and are not to be considered in the construction or interpretation of any provision of the Agreement. Any exhibit, document or schedule referred to in the Agreement means such exhibit or schedule as amended, supplemented and modified from time to time to the extent permitted by the applicable provisions thereof and by the Agreement. References to any statute or regulation mean such statute or regulation as amended at the time and includes any successor statute or regulation. Unless otherwise stated, references to recitals, sections, subsections, paragraphs, schedules and exhibits will be references to recitals, sections, subsections, paragraphs, schedules and exhibits of the Agreement. All dollar amounts in the Agreement are in U.S. currency unless otherwise indicated.

35. **Counterparts.** This document may be executed simultaneously in two (2) or more counterparts, each of which will be considered an original, but all of which together will constitute one and the same instrument.

[END OF GENERAL TERMS AND CONDITIONS]

PROFESSIONAL SERVICES OFFERING SCHEDULE

The Agreement for Entrust's Professional Services is comprised of this Schedule, the Entrust General Terms and Conditions and an Order for Professional Services. Capitalized terms not defined herein have the meanings given to them in the General Terms.

1.1. Schedule. The actual start and completion dates of the Professional Services are dependent upon Entrust resource availability and Customer resource availability. Upon agreement by the parties of a start date for the Professional Services and provided that Entrust resources have been confirmed to Customer, in the event Customer cancels or reschedules such Professional Services by notifying Entrust less than five (5) business days prior to the agreed upon start date, Customer will reimburse Entrust for the costs incurred by Entrust due to Customer's cancellation or rescheduling.

1.2. Professional Services Hours and Travel. Unless otherwise provided in the Order, the Professional Services will be provided on a time and materials basis. The Order will set out, if and as applicable, the number of hours in a working day, the specialists, their per diem rates, their estimated level of effort and their estimated fees. Fees are calculated to the nearest hour. Actual, reasonable travel and living expenses and out-of-pocket expenses, if any, are not included in the Professional Services fees and will be invoiced separately in accordance with FAR 31.205-46 and the Federal Travel Regulation (FTR). Customer shall only be liable for such travel expenses as approved by Customer and funded under the applicable ordering document.

1.3. Background and Professional Services IP. Any intellectual property rights of a party or its Affiliates conceived, created, developed, or reduced to practice prior to, or independently of, any Professional Services provided under the Agreement ("Background IP") shall remain the exclusive property of such party or its Affiliate. Customer grants Entrust a non-exclusive, non-transferable, royalty-free, worldwide license for the term of the applicable Order to make, use and copy any Customer Background IPR that it discloses to Entrust, but solely to the extent necessary for Entrust to provide the Professional Services to the Customer pursuant to the Order. The Professional Services, including all deliverables, are not "works for hire", and the intellectual property embodied therein is owned by Entrust ("Professional Services IP"). Entrust grants Customer a non-exclusive, non-transferable, royalty-free, worldwide, perpetual license to any Professional Services IP incorporated into a deliverable, but solely to the extent necessary to use and exploit the deliverable as contemplated in the applicable Order and only so long as such Professional Services IP is embedded in the deliverable and not separated therefrom.

1.4. If required, Customer will provide on-site working space for the Entrust Professional Services team. Customer shall take all steps reasonably necessary to ensure the health and safety of the employees and subcontractors of Entrust and its Affiliates when such personnel are on Customer sites and Customer shall advise such personnel of the rules and regulations governing their conduct at Customer sites.

1.5. Customer project staff shall have sufficient availability to participate in the Professional Services as is required by Entrust staff, for example, answering technical questions, availability for meetings, and other general questions as they may arise.

SCHEDULE

DATA PROCESSING ADDENDUM (DPA)

ENTRUST ACTING AS PROCESSOR - GLOBAL

DATA PROCESSING

This Data Processing Addendum ("**DPA**") supplements and forms part of the written or electronic agreement(s) (individually and collectively the "**Agreement**") between Entrust (as defined below) and Customer (as defined below) for the purchase, access to, and/or licensing of products, services and/or platforms (collectively the "**Services**") to reflect the parties' agreement with regard to the Processing of Personal Data. The terms used in this DPA shall have the meanings set forth in this DPA. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement. Except as modified in the DPA, the terms of the Agreement shall remain in full force and effect.

If the Customer is an Ordering Activity under GSA Schedule Contracts, it shall only be required to comply with the Federal law of the United States and expressly does not agree to comply with any provision of this Data Processing Agreement, EU Law, or law of an EU Member State that is inconsistent with the Federal law of the United States.

1. INSTRUCTIONS

1.1. This DPA has been pre-signed on behalf of Entrust Corporation, acting for itself and for and on behalf of its Affiliates. To enter into this DPA, the Customer must:

1.1.1. Have a written or electronic agreement with Entrust;

1.1.2. Complete the Customer point of contact requested in Section 9.1.

1.1.3. Complete the signature block below by providing the name of the signatory, their signature, their position, the address of the Customer, and the date the DPA was executed; and

1.1.4. Submit the completed and signed DPA to Entrust at privacy@entrust.com.

2. EFFECTIVENESS

2.1. This DPA will only be effective (as of the Effective Date) if executed and submitted to Entrust accurately and in full accordance with paragraph 1 above and this paragraph 2. If Customer makes any deletions or other revisions to this DPA which are not explicitly agreed to by Entrust, this DPA will be deemed null and void.

2.2. This DPA shall be effective for the duration of the Agreement (or longer to the extent required by applicable law).

2.3. The parties agree that this DPA shall replace any existing DPA or other contractual provisions pertaining to the subject matter contained herein that the parties may have previously entered into in connection with the Services, and will be effective as of the date Entrust receives a complete and executed DPA from the Customer indicated in the signature block below.

3. DEFINITIONS

"**Controller**" is synonymous with "personally identifiable information controller" as such terms are defined in the Data Protection Laws and in ISO 27701 and refers to the entity that determines the purpose and means of Processing Personal Data.

"**Customer**" means an existing or potential customer of Entrust.

"**Data Protection Laws**" refers toall applicable data protection and data privacy laws and regulations, including, but not limited to, the EU General Data Protection Regulation (GDPR), UK General Data Protection Regulation (UK GDPR), Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) and the California Consumer Privacy Act (CCPA).

"**Data Subject**" is synonymous with "personally identifiable information principal" as such terms are defined in the Data Protection Laws and in ISO 27701 and refers tothe identified or identifiable person or household to whom Personal Data relates.

"**Entrust**" means the Entrust Corporation entity that is a party to the Agreement.

"**Personal Data**" shall have the meaning ascribed to "personally identifiable information," "personal information," "personal data" or equivalent terms as such terms are defined in the Data Protection Laws and in ISO 27701.

"**Personal Data Incident**" shall have the meaning assigned in the Data Protection Laws to the terms "security incident," "security breach" or "personal data breach" and shall include any situation in which Entrust becomes aware that Personal Data has been or is likely to have been accessed, disclosed, altered, lost, destroyed or used by unauthorized persons, in an unauthorized manner.

"**Processing**" means any operation or set of operations that is performed on Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"**Processor**" is synonymous with "personally identifiable information processor" as defined in ISO 27701 and refers to the entity that Processes Personal Data on behalf of the Controller.

"EU Standard Contractual Clauses" means the contractual clauses set out in Schedule 2, amended as indicated (in square brackets and italics) in Schedule 2 and as otherwise amended, superseded, or replaced from time to time in accordance with this DPA.

"**Sub-processor**" means any entity appointed by the Processor to Process Personal Data on behalf of the Controller.

4. PERSONAL DATA PROCESSING

4.1. **Roles of the Parties**. The parties acknowledge and agree that with regard to the Processing of Personal Data under the Agreement, Customer is the Controller and Entrust is the Processor.

4.2. **Customer's Instructions for the Processing of Personal Data.** Customer's instructions for the Processing of Personal Data shall comply with Data Protection Laws. Customer shall have sole responsibility for the accuracy, quality, and legality of Personal Data and the means by which Customer acquired Personal Data.

4.3. **Entrust's Processing of Personal Data**. Entrust shall only Process Personal Data on behalf of and in accordance with Customer's instructions and for the following purposes: (i) Processing for the specific purpose of performing the services specified in the Agreement or as otherwise required by law; and (ii) Processing to comply with other documented reasonable instructions provided by Customer where such instructions are consistent with the terms of the Agreement. Entrust shall immediately inform Customer if, in Entrust's opinion, an instruction is in violation of Data Protection Laws. For the avoidance of doubt, Entrust will not collect, retain, use, sell, or otherwise disclose Personal Data for any purpose other than for the specific purpose of performing the Services or as otherwise required by law.

4.4. **Details of the Processing.** The subject matter of Processing of Personal Data by Entrust is the performance of the Services pursuant to the Agreement. The duration of the Processing, the nature and purpose of the Processing, the types of Personal Data Processed and the categories of Data Subjects for whom Personal Data is Processed are set forth in Schedule 1.

4.5. **Personnel**. Entrust shall ensure only authorized personnel who have undergone appropriate training in the protection and handling of Personal Data, and are bound in writing to respect the confidentiality of Personal Data, have access to Personal Data.

4.6. **Security Controls**. Entrust shall implement appropriate technical and organizational measures to maintain the security, confidentiality and integrity of Personal Data, including measures designed to protect against unauthorized or unlawful Processing and against accidental or unlawful destruction, loss or alteration or damage, unauthorized disclosure of, or access to, Personal Data.

4.7. **Data Subject Requests.** Entrust shall, taking into account the nature of the Processing, assist the Customer, as Data Controller, by appropriate technical and organizational measures, insofar as this is possible, in fulfilling the Customer's obligation to respond to requests from a Data Subject exercising his/her/their rights under Data Protection Laws.

4.8. **Data Protection Impact Assessment.** Entrust shall, upon Customer's written request and taking into account the nature of Processing and information available, provide reasonable assistance to Customer in connection with obligations under Articles 32 and 36 of the GDPR or equivalent provisions under Data Protection Laws.

4.9. **Return or Deletion of Personal Data.** Entrust shall, upon Customer's written request, promptly destroy, anonymize or return any Personal Data after the end of the provision of Services, unless storage of the Personal Data is required by applicable law.

4.10 **Data Processor Point of Contact**. If Customer has any questions regarding Processing of Personal Data by Entrust, Customer may send such questions to the following email: privacy@entrust.com.

5. HIPAA

5.1. If Customer is a “covered entity” under the Health Insurance Portability and Accountability Act (HIPAA) and Entrust will process "protected health information" as a “business associate” as these terms are defined in 45 CFR § 160.103, execution of this DPA includes execution of the HIPAA Business Associate Agreement (“BAA”), the full text of which is available at https://www.entrust.com/legal-compliance/data-privacy. The BAA can only be used with “HIPAA-Covered Services” as those are defined at https://www.entrust.com/legal-compliance/data-privacy. Customer may opt out of the BAA by sending the following information to privacy@entrust.com:

- the full legal name of the Customer that is opting out; and
- if Customer has multiple Agreements, the Agreement to which the opt out applies.

6. SUB-PROCESSORS

6.1. **Appointment of Sub-processors**. Customer acknowledges and agrees that Entrust may engage Sub-processors in connection with provision of the Services. Entrust shall enter into a written agreement with any engaged Sub-processor that contains data protection obligations no less protective than those contained in this DPA.

6.2. **List of Current Sub-processors**. The current list of Sub-processors for the Services can be found at www.entrust.com/sub-processors.

6.3. **Notification of New Sub-processors.** Entrust will notify Customer in writing of any changes to this list of Sub-processors.

6.4. **Objection to New Sub-processors**. Customer may object to Entrust’s use of a new Sub-processor by notifying Entrust in writing within ten (10) business days after receipt of Entrust’s communication advising of the new Sub-processor. In the event Customer reasonably objects to the use of a new Sub-processor, Entrust will use reasonable efforts to address Customer’s objections. If Entrust is unable to make available such change within a reasonable period, which shall not exceed ninety (90) days, Customer may terminate the applicable Agreement with respect only to those Services which cannot be provided by Entrust without the use of the objected-to new Sub-processor by providing written notice to Entrust. Entrust will refund Customer any prepaid fees covering the remainder of the term of such Agreement following the effective date of termination with respect to such terminated Services, without imposing a penalty for such termination on Customer.

6.5. **Liability.** Entrust shall be liable for the acts and omissions of its Sub-processors to the same extent Entrust would be liable if performing the services of each Sub-processor directly under the terms of this DPA, except as otherwise set forth in the Agreement.

7. PERSONAL DATA INCIDENTS

7.1. Entrust shall notify Customer without undue delay after becoming aware of a Personal Data Incident. Entrust shall identify the cause of such Personal Data Incident and take those steps reasonably necessary in order to remediate the cause of such a Personal Data Incident.

8. INTERNATIONALDATA TRANFERS

8.1. **Personal Data Transfers**. Customer agrees to allow transfer of Personal Data outside the country from which it was originally collected provided that such transfer is required in connection with the provision of Services under the Agreement and such transfers take place in accordance with Data Protection Laws, including, without limitation, completing any prior assessments required by Data Protection Laws.

8.2. **European Specific Provisions.** Where Entrust transfers Personal Data collected in the European Economic Area to a country outside of the European Economic Area and without an adequacy finding under Article 45 of the GDPR, Entrust shall transfer Personal Data pursuant to the EU Standard Contractual Clauses as set forth in Schedule 2. The EU Standard Contractual Clauses are hereby incorporated in their entirety into this DPA and, to the extent applicable, Entrust shall ensure that its Sub-processors comply with the obligations of a data importer (as defined in the EU Standard Contractual Clauses). To the extent there is any conflict between this DPA and the EU Standard Contractual Clauses, the terms of the EU Standard Contractual Clauses shall prevail.

9. CERTIFICATIONS AND AUDITS

9.1. On no more than an annual basis and upon thirty (30) days' notice in writing by Customer, Entrust, to the extent that it is acting as a Data Processor to Customer, shall make available to Customer information necessary to demonstrate compliance with the obligations set forth under Data Protection Laws, provided that Entrust shall have no obligation to provide confidential and/or proprietary information. On no more than an annual basis and upon thirty (30) days' notice in writing, Entrust shall, to the extent that it is acting as a Data Processor to Customer, following a request by Customer and at Customer's expense, further allow for and contribute to off-site audits and inspections by Customer or its authorized third- party auditor. The scope, timing, cost and duration of any such audits, including conditions of confidentiality, shall be mutually agreed upon by Entrust and Customer prior to initiation. Customer shall promptly notify Entrust with information regarding non-compliance discovered during the course of an audit, and Entrust shall use commercially reasonable efforts to address any confirmed non-compliance.

10. Notice

10.1. Any notice required by Entrust to Customer under this Addendum shall be sent to ______________________________.

List of Schedules

Schedule 1: Details of the Processing

Schedule 2: EU Standard Contractual

Clauses

The parties' authorized signatories have duly executed this DPA:

On behalf of Customer:

Customer Name: ______________________________

Name (written out in full): ______________________________

Position: ______________________________

Address: ______________________________

Signature: ______________________________

Date: ______________________________

On behalf of Entrust:

Name (written out in full): **Lisa J. Tibbits**

Position: **Chief Legal and Compliance Officer**

Address: **1187 Park Place, Shakopee, Minnesota 55379-3817 USA**

Signature: Lisa J Tibbits______________________________

SCHEDULE 1 - DETAILS OF PERSONAL DATA PROCESSING

Nature and Purpose of Processing

Entrust will Process Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Services-related documentation, and as further instructed by Customer in its use of the Services.

Duration of Processing

Entrust will Process Personal Data for the duration of the Agreement, unless otherwise agreed upon in writing or as required by applicable laws.

Categories of Data Subjects

Customer may submit Personal Data to Entrust, the extent of which is determined and controlled by Customer in its sole discretion (but in accordance with Data Protection Laws), and which may include, but is not limited to Personal Data relating to the following categories of data subjects:

- Customer's employees, clients, agents and subcontractors
- Customer's end users authorized by Customer to use the Services
- *See also* the relevant product privacy notice

Categories of Personal Data

Customer may submit Personal Data to Entrust, the extent of which is determined and controlled by Customer in its sole discretion (but in accordance with Data Protection Laws), and which may include, but is not limited to the following categories of Personal Data:

- Business contact details (name, title/position, address, telephone number, fax number, email address, location) of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- Connection data (IP address, username, ID data used for authentication purposes) of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- Biometric data of Customer's employees, clients, agents, subcontractors and end users authorized by Customer to use the Services
- *See also* the relevant product privacy notice

SCHEDULE 2 – EU STANDARD CONTRACTUAL CLAUSES (Controller to Processor)

Clause 1

Purpose and scope

a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)[1] for the transfer of personal data to a third country.

b) The Parties:

   i. the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter "entity/ies") transferring the personal data, as listed in Annex I.A. (hereinafter each "data exporter"), and

   ii. the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A. (hereinafter each "data importer")

   have agreed to these standard contractual clauses (hereinafter: "Clauses").

c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B

d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46 (2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

[1] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protectionobligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses includedin Decision 2021/915.

b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

   i. Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

   ii. Clause 8.1(b), 8.9(a), (c), (d) and (e);

   iii. Clause 9(a), (c), (d) and (e);

   iv. Clause 12(a) and (d) and (f);

   v. Clause 13;

   vi. Clause 15.1(c), (d) and (e);

   vii. Clause 16(e);

   viii. Clause 18(a) and (b);

b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter ‘personal data breach’). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union [2] (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

i. the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;
ii. the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;
iii. the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or
iv. the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.
b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.
c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

[2] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least thirty (30) days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. [3] The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

[3] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

    i. lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

    ii. refer the dispute to the competent courts within the meaning of Clause 18.

d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

a) The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

   i. the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

ii. the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards [4];

iii. any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

[4] As regards the impact of suchlaws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal recordsor other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this informationcan be lawfully sharedwith thirdparties. Where this practical experience is reliedupon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroboratedand not contradictedby publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

   i. receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

   ii. becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

   i. the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

   ii. the data importer is in substantial or persistent breach of these Clauses; or

   iii. the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

   In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of the EU Member State in which the data exporter is established. Where such law does not allow for third-party beneficiary rights, they shall be governed by the law of another EU Member State that does allow for third-party beneficiary rights. The Parties agree that this shall be the law of Ireland.

Clause 18

Choice of forum and jurisdiction

a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

b) The Parties agree that those shall be the courts of Ireland.

c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

d) The Parties agree to submit themselves to the jurisdiction of such courts.

ANNEX I TO THE STANDARD CONTRACTUAL CLAUSES

A. List of Parties

Data exporter

The data exporter is Customer.

Data importer

The data importer is the Entrust legal entity Customer has an Agreement with.

B. Description of Transfer

Data subjects

The personal data transferred concern the following categories of data subjects:

- See Schedule 1

Categories of data

The personal data transferred concern the following categories of data:

- See Schedule 1

Frequency of the transfer

The personal data will be transferred on a continuous basis.

Nature and purpose of the processing

The personal data transferred will be subject to the following basic processing activities:

- The performance of the Services pursuant to the Agreement

Retention period

The personal data will be retained for the duration of the Agreement or longer if required by law.

Sub-processor transfers

The subject matter, nature and duration of processing by sub-processors is as follows:

https://www.entrust.com/legal-compliance/data-privacy/sub-processors.

C. Competent Supervisory Authority

The supervisory authority of Ireland with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer shall act as competent supervisory authority.

ANNEX II TO THE STANDARD CONTRACTUAL CLAUSES

This Annex forms part of the Clauses and has been agreed by the parties by virtue of their signing the DPA.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

Reliability of Personnel: To the extent permitted by law, Entrust conducts background checks on all employees before employment, and employees and contractors receive information security training during onboarding as well as on an annual basis. All employees are required to read and sign Entrust's information security policies.

Compliance, audits, and certifications: Entrust, with the full commitment of its senior leadership, strongly believes that the fundamental principle to its success in innovation is its information security strategy. This strategy is based on adherence to enterprise-wide governance, a set of controls and strict compliance with federal, financial, international, and industry regulations and policies. Entrust's corporate information security management system (ISMS) is ISO 27001 compliant. Additionally, Entrust maintains compliance certifications to various other standards and frameworks, depending on the product, service, and geographic location, including:

- ISO 27701
- ISO 9000
- ISO 14000
- PCI CP
- PCI SAQ
- CAIQ Cloud Security Alliance
- Webtrust – CAB Forum
- NIST/FISMA
- NIST 800-53
- ETSI
- Tscheme

To ensure that the information security strategy is effective, Entrust enforces information security policies and procedures across its entire organization, as well as all business and technical projects. Governance, Risk and Compliance (GRC), Threat and Vulnerability Management (TVM), Security Architecture, Security Operations Center, Disaster Recovery, Business Continuity and Incident Response are the integral components of this strategy.

Incident Response:

At an operational level, Entrust has instituted a Security Incident Response Plan to oversee data security events identified or detected by the various technologies used to monitor and alert based on specific thresholds or circumstances. The objectives of the Security Incident Response Plan are to manage and coordinate data security incidents throughout all aspects of the Entrust computing environment regardless of location, product or process, as well as provide opportunities for educating our colleagues on risks and security controls in place.

Security Operation Center (SOC):

Entrust is committed to protecting the interest of stakeholders by maintaining a robust Security Operation Center (SOC). The SOC is a centralized unit that monitors the confidentiality, integrity, and availability of information technology infrastructure and deals with security on an organizational level.

Threat and Vulnerability Management (TVM):

Entrust has a continuous vulnerability discovery and remediation program. This process is built on industry certified tools and procedures and is facilitated by competent and experienced professionals. The Threat and Vulnerability Management (TVM) controls and measures are audited several times a year by qualified auditors to ensure we are compliant with applicable laws and industry standard frameworks.

Disaster Recovery:

Entrust is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust therefore maintains a comprehensive organization-wide business continuity program to protect staff, safeguard corporate assets and environments, and to ensure continuous availability of its products and services. To support the Business Continuity Program, Entrust also maintains a Crisis Communications and Incident Response Plan to help strengthen our emergency response capability.

Business Continuity:

Entrust is committed to protecting the interest of stakeholders in the event of an emergency or business disruption. Entrust therefore maintains a comprehensive organization-wide Business Continuity Program that is consistent with the guidance issued by the (U.S.) National Fire Protection Association (NFPA) 1600 – Standard on Disaster/Emergency Management and Business Continuity Programs, and (International) ISO 22301 – Societal security – Business continuity management systems standards. The Business Continuity Plan identifies the functional roles and responsibilities of internal and external agencies, organizations and departments.

Systems and Product Acquisitions, Development and Maintenance:

Entrust's information security program includes policies, standards, and processes for System Development Lifecycle (SDLC) that are aligned with industry recognized practices for the secure management of systems throughout their lifecycle. Phases of the SDLC includes: Requirements, Design, Implementation, Testing, Deployment, Operations, Maintenance, and Retirement. . Vulnerability identification and remediation are a central focus with the goal to minimize the number of security flaws in Entrust products and services, and to minimize the impact to Customer when such flaws are discovered. The processes described herein apply to Entrust products and services and components of a partner system that may be used in conjunction with an Entrust product or service. The program will ensure that SDLC processes are consistent with Entrust information security goals and expectations. Additionally, system baselines will be established to support Entrust software and firmware within the lifecycle (e.g., source repositories) and to support deployment into production environments. Where practical, system baselines will be aligned with compliance requirements.

Network Security:

Entrust maintains access controls and policies to manage what access is allowed to the Entrust network and systems from each network connection and user, including the use of firewalls or functionally equivalent technology and authentication controls. Entrust will maintain corrective action and incident response plans to respond to potential security threats.

Physical and Environment Security:

Entrust facilities hosting technology information assets are equipped with appropriate controls to restrict physical access to the facility. Physical entry controls include a means to identify personnel and visitors, and ensure the individual is authorized to access the secured area prior to entry. All entry to secured areas are logged and logs are reviewed periodically. Personnel are informed of, and subject to, the guidelines established for working within secured areas. Access points such as delivery or loading areas, and other points where unauthorized persons may enter the facility, are controlled to restrict further entry, and, to the extent it is practical, isolated from information processing areas. Physical security measures include the capability to monitor company facilities to detect unauthorized or unlawful use. Entrust has a physical security plan that incorporates a defined procedure to report suspicious activity, identified security weaknesses, or potential security events, as well as an escalation procedure to communicate events to local law enforcement as appropriate. Facility staff and visitors are informed regarding these physical security procedures and their responsibility to report security events.

Information Transfer Policy:

Information to be transferred shall at all times be properly secured, in accordance with its classification, regardless of the media employed to carry the information or the transmission mechanism. All information to be transferred shall be subject to inspection for malicious software code and other potential hazards to confidentiality, integrity or availability. When the use of encryption is required for safekeeping, such use shall be subject to all applicable security controls as well as legal or regulatory requirements. Information to be transferred shall be subject to established retention and disposal requirements. Information transfer facilities shall comply with all applicable laws and regulations. Information and software shall not be transferred with external parties until all relevant contractual and security requirements are satisfied, including formal written agreements where required.

Third-Party Management:

Entrust’s third-parties, such as vendors, subcontractors, sub-processors, and service providers, that have access to data, information, facilities, or impact Entrust’s products or services are continuously managed, monitored, reviewed, and bound to uphold high standards for privacy and information security. Third-parties are periodically assessed based on the sensitivity of their level of access to systems and information as well as the criticality of their services. Entrust limits access to third-parties on a “need to know” basis and revokes when it is no longer needed

Hardware and Supplies Schedule

If Entrust provides any Hardware and Supplies in connection with an Order, then the following terms apply with respect to the Hardware and Supplies portion of the Offering. Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Shipment; Title and Risk of Loss.** Unless otherwise specified in this Agreement: (i) Hardware and Supplies will be shipped at Entrust's sole discretion either EXW Entrust's dock or FCA Entrust's dock ("INCOTERMS 2020"): (ii) Customer is responsible for obtaining all insurance needed and for all shipping charges; (iii) Hardware and Supplies are deemed to be accepted by the Customer upon delivery in accordance with the INCOTERMS 2020 stated above; and (v) Customer is responsible for installation of the Hardware and Supplies. Legal title and risk of loss of or damage to the Hardware and Supplies pass from Entrust to Customer upon delivery to the shipping carrier in accordance with the applicable INCOTERMS 2020.

2. **Warranties.** Entrust makes no warranties with respect to the Hardware and Supplies or Software associated to Hardware and Supplies other than as set forth in this Schedule or as may be set forth in the documentation delivered by Entrust with the Hardware and Supplies ("Warranty Documentation"), which warranties are subject to the limitations set forth in this paragraph. Entrust warrants that i) Software associated to Hardware and Supplies will perform in accordance with specification set out in the related Documentation for a period of ninety (90) days from the date of delivery; and ii) Hardware and Supplies will be free from defects in material and workmanship for one year unless otherwise set forth in the Warranty Documentation. The remedy for breach of the aforesaid warranty is limited to the repair or replacement of the defective item at no charge to Customer or the refund of the purchase price of the item, at Entrust's sole option, and is conditioned upon (i) Customer's payment of the price or fee specified in an applicable Order (except for purchases via authorized resellers); (ii) the proper use, maintenance, management and supervision of the item; (iii) the exclusive use of Hardware and Supplies or consumable materials supplied by Entrust for the item; (iv) a suitable operating environment for the item; and (v) the absence of any intentional or negligent act or other cause external to the item affecting its operability or performance. This warranty will be null and void if maintenance is performed on a Hardware and Supplies by any party other than Entrust or a qualified party approved by Entrust or if any addition to, removal from or modification of the Hardware and Supplies is made without Entrust's approval. Once they have been replaced, all parts removed from Hardware and Supplies under warranty will become the property of Entrust. If Entrust is requested to provide maintenance service for the Hardware and Supplies that is not covered by the stated warranty, Customer will be responsible for the cost of all such service at Entrust's then-current time and materials rates.

3. **Waste Electrical and Electronic Equipment.** For sales made in the European Union, the Customer alone shall be responsible for, and shall bear the cost of the collection, treatment, recovery and environmentally sound disposal of waste electrical and electronic equipment for the purposes of any decree, statute, regulations, order or other legislation which implements the terms of Directive 2012/19/EU on Waste Electrical and Electronic Equipment in the member state concerned.

4. **Software (and Firmware) License Associated to Hardware and Supplies.** Customer's rights related to Software (and Firmware) Associated to Hardware and Supplies are established by and limited to the terms and conditions specified in the End User License Agreement (EULA) accompanying the Hardware and attached hereto.

5. **Support**. Entrust provides the service levels and Support Services for the Hardware and Supplies (including Software Associated to Hardware and Supplies) as set out in the Support Schedule or a separate Support agreement, a copy of which is available at request. Where Support is purchased through an authorized reseller and the Order indicates that the reseller will provide Support, such support will be provided by the authorized reseller.

6. **Issuance HSM**. If Customer has purchased an Issuance HSM, Customer is strictly prohibited from using the Issuance HSM as a general purpose HSM and may only use the Issuance HSM for the limited purposes of supporting Entrust's 'Issuance' products. An "Issuance HSM" means a hardware security module ("HSM") that that has been purchased and/or licensed specifically for supporting Entrust's credit card Issuance products.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. "**Business Day**" means any day other than Saturday, Sunday, or a public holiday.

1.2. "**Covered Offering**" means each Hardware, Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support.

1.3. "**Customer-Hosted Offering**" means Hardware, Software, and/or Third Party Vendor Products that are hosted by Customer or installed on Customer's premises.

1.4. "**Discretionary Extended Support**" means the services which may be available from Entrust under a separate agreement, for End of Support Products or non-standard support relating to reinstatement of Support.

1.5. "**End of Support Product**" means a previous version of Hardware, Software that has entered the End of Support phase as set out in the *Entrust Data Protection Solutions Support Lifecycle Policy* (available upon request), or a Third Party Vendor Product that is no longer supported (as set out in the relevant Documentation for such product).

1.6. "**Hardware**" for the purposes of this Schedule means any "Hardware and Supplies" (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.7. "**Hosted Service**" for the purposes of this Schedule means nShield as a Service Direct (nSaaS Direct).

1.8. "**Named Support Contacts**" means individual Users nominated by Customer to act as Customer's support representatives.

1.9. "**Problem**" means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.10. "**Production Environment**" means Customer's live business environment with active users.

1.11. "**Response Time**" means the amount of time that elapses between the Customer's report of a Service Request to Entrust and Entrust's acknowledgement of the report, confirmation or assignment of a severity or priority classification, and indicating that a response to the Problem or request has been initiated.

1.12. "**Service Plan**" means the applicable Service Plan for the Covered Offering as referenced in the Support Welcome Pack.

1.13. "**Service Request**" means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.14. "**Software**" for the purposes of this Schedule means any Software (as defined in the General

Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Discretionary Extended Support.

1.16. "**Support Welcome Pack**" means guide to using Support Services for the applicable Covered Offerings containing, inter alia, information related to the relevant Service Plans.

1.17. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

4. **Support Fees.**

4.1. Fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5. **Customer's Named Support Contacts**.

5.1. When making a Service Request, Customer shall provide:

5.1.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

5.1.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

5.1.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

5.2. For Severity 1 Problems, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Problem. If no dedicated Customer resources are available, Entrust's obligations with respect to the Problem will be suspended until such time as such resources become available.

5.3. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

6. **Support Services For Third Party Vendor Products.**

6.1. Support for Third Party Vendor Products.

6.1.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

6.1.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

6.1.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7. **Upgrades for Customer-Hosted Offerings**.

7.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, and unless otherwise specified, Entrust will have no obligation to provide Support Services for End of Support Products. Entrust may offer to provide Discretionary Extended Support for such End of Support Products for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Discretionary Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

7.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. "for Windows") and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. "for Mac"), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

8. **Exclusions**.

8.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer's failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported Covered Offerings (including, without limitation, End of Support Products), or (h) with respect to Hardware, an act or omission of Customer related to relocation, movement, or improper installation with reference to the installation Documentation.

8.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer's use of the Covered Offering shall be at Customer's own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

8.3. This Support Schedule expressly excludes on-site support and support for (a) any Covered Offering that was provided on a "no charge", beta testing, proof of concept, evaluation or "not for resale" basis, (b) for hardware other than Hardware, (c) for third party products and services other than Covered Offerings, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

9. <u>Support Services.</u>

9.1. DPS Cloud Security, Encryption and Key Management (formerly "Hytrust") Software

9.1.1 Help Desk Support. Telephone (+1 (844) 681-8100), email (hytrust.support@entrust.com) and web-based (https://my.hytrust.com) support will be provided to Named Support Contacts (as noted below) between the hours of 5:00 a.m. and 5:00 p.m. Pacific Time, Monday through Friday. Emergency support for Severity 1 Problems will be available twenty-four/seven (24/7/ 365) by contacting: toll-free +1 (844) 681-8100 or creating a Severity 1 case at https://my.hytrust.com. Customer will designate up to three (3) Named Support Contacts and provide their names to Entrust. Only Named Support Contacts may raise a Service Request.

9.1.2 Problem Correction & Service Levels. Each Service Request related to the Software covered by Section 9.1 that has been submitted by Named Support Contact will be issued a tracking number and will be tracked by Entrust. Entrust may acknowledge submission of each Service Request through automated means (e.g. automated response email) or by direct contact via email or phone by an Entrust technical representative within the response times set out below for the applicable severity level. 'Severity Level' is a measure of the relative impact of an issue on Customer's systems or business. Entrust and Named Support Contact will work together to accurately define the severity level for a Service Request.

Severity Level	Impact	Initial Response by Entrust

Severity 1	Software is completely inoperative or at least one component of mission-critical functionality does not perform.	Within one (1) hour. Error diagnosis to commence immediately.
Severity 2	The overall performance of Software is degraded or at least one component of material (but not mission-critical) functionality does not perform.	Within four (4) hours. Error diagnosis to commence immediately.
Severity 3	Any Problem that affects performance of the Software but does not degrade any material or mission critical functionality.	Within twelve (12) hours. Error diagnosis to commence immediately.
Severity 4	General questions, feature requests, etc.	Within twelve (12) hours.

9.1.3 Lapsed Support Services Reinstatement. In the event Support Service expires or is otherwise terminated: (i) any reinstatement of Support Service shall be purchased to cover the lapsed Support Service since expiration or cancelation and must be renewed until the Support Service is current. In addition, Customer shall warrant that as of the date of the order for renewal is placed that (to the best of its knowledge) all Software covered under this Section 9.1 are functioning correctly. Reinstatement for lapsed Support Services can be backdated to a maximum of eighteen (18) months.

9.1.4 Supported Versions and End Of Life. Unless otherwise specified by Entrust, the provision of Support Services under this Section 9.1 do not apply to End of Support Products. The list of currently supported versions is available on request from the Entrust technical support team.

9.2. **Hosted Service**

9.2.1. Support Services. The availability of Support Services for nSaaS Direct is set out in the Support Welcome Pack available at https://www.entrust.com/-/media/documentation/userguides/dps- nshieldaas-welcome-kit-br.pdf.

9.3. **Hardware Security Modules (nShield HSMs and related Software - excluding products covered under Section 9.1 and 9.2)**

9.3.1. Support Services. The availability of Support Services for Hardware and Software covered under this Section 9.3 is set out in the Support Welcome Pack available at https://www.entrust.com/-/media/documentation/brochures/customer-welcome-pack-technical-support- br.pdf . Entrust will use commercially reasonable efforts to meet the response times noted in the Welcome Pack. Access to the Support Help Center, e-mail or phone lines for the provision of Support may be suspended for brief periods due to scheduled maintenance and other factors. “Support Help Center” means the Entrust nShield Technical Support Help Center that can be accessed from the following link https://www.entrust.com/contact/support.

9.3.2. Lapsed Support Services Reinstatement. In the event Support Service expires or is otherwise terminated: (i) any reinstatement of Support Service shall be purchased to cover the lapsed Support Service since expiration or cancelation and must be renewed until the Support Service is current. In addition, Customer shall warrant that as of the date of the order for renewal is placed that (to the best of its knowledge) all Hardware and Software covered under this Section 9.3 are functioning correctly. Reinstatement for lapsed Support Services can be backdated to a maximum of eighteen (18) months.

9.3.3. Supported Versions and End Of Life. Unless otherwise specified by Entrust, the provision of Support Services under this Section 9.3 do not apply to End of Support Products. The *Entrust Data Protection Solutions Support Lifecycle Policy* defines currently supported versions and is available on request from the Entrust technical support team.

9.3.4. Hardware.

9.3.4.1. Service Plan Options:

9.3.4.1.1. Repair Replacement Option (Standard Support): During an active Support Services term, where the Service Plan purchased by Customer includes the *Repair/Replacement* option, Entrust will repair the original unit or, will ship a replacement unit following receipt of Customer's report and acknowledgement by Entrust that the Hardware in the Order has experienced a Problem which is covered by the Support Services under Section 9.3. Entrust will ship the repaired or replacement unit within fifteen (15) Business Days after receipt at the location specified on the return material authorization ("**RMA**").

9.3.4.1.2. Advance Replacement Option (Premium and Premium Plus Support): During an active Support Services term, where the Service Pan purchased by Customer includes the *Advanced Replacement* option, Entrust will make reasonable efforts to ship a replacement unit by the end of the next Business Day following receipt of Customer's report and acknowledgement by Entrust (report must be received, along with confirmation of Named Support Contact contact details, including name, address, email, and phone number, by 12pm local time for the relevant Entrust support team, failing which the replacement unit will be shipped one the subsequent Business Day – i.e. two Business Days following receipt) that a Product set forth in the Order has experienced a Problem which is covered by Support Services under Section 9.3.

9.3.4.1.3. Rapid Delivery For UK Mainland and On-Site Spare Service Options: During an active Support Services term, where the Service Pan purchased by Customer includes *Rapid Delivery* (available for UK mainland only) or the *On-Site Spare* options, Entrust will, within four (4) operational hours (of a Business Day) of notification that a Hardware unit covered by *Rapid Delivery* support has experienced a Problem and requires replacement, dispatch a support engineer with a replacement Hardware unit. For the *On-Site Spare* option the Customer shall be responsible for holding an additional spare at each of its allocated sites. The Customer is responsible for ensuring that the unit that has experienced a Problem is made available for collection by the support engineer when the replacement Hardware unit is delivered. Customer is responsible for informing Entrust of the location of all units covered by either the *Rapid Delivery* or the *On-Site Spare* option and for informing Entrust of any changes to the locations of the units. Where Customer has used its site Hardware unit spare under the *On-Site Spare* option it shall be accountable for immediately notifying Entrust's technical support team in order that arrangements can be made (with no additional cost to the Customer) to collect the faulty Hardware unit and provision a new Hardware unit that can respectively be stored at Customer's site. The *Rapid Delivery* and *On-Site Spare* options do not include the installation, de-installation or removal of the Hardware units.

9.3.4.2. Hardware Return Material Authorization Policy

9.3.4.2.1. Prior to returning any Hardware to Entrust for repair or replacement, Customer must ensure that: the Hardware is free of any legal obligations or restriction and of any Customer proprietary or confidential information that would prevent Entrust from exchanging, repairing or replacing the Hardware; Customer has obtained a RMA from Entrust, including a RMA number; and it has complied with all applicable export and import control requirements. Certain Hardware components are considered non-returnable items – including, without limitation, smart cards, cables, and rail kits (each "**Non-Returnable Items**"). For a full list of Non-Returnable Items, Customer should contact Entrust technical support prior to the return. Entrust cannot guarantee delivery of any Non-Returnable Items back to the Customer. Export control requirements may require Entrust to provide the full price book value of the Hardware components on Documentation accompanying the RMA shipment.

9.3.4.2.2. All returns must comply with any Entrust RMA instructions set out in the Support Welcome Pack or as advised by Entrust personnel. If Customer does not follow all Entrust RMA instructions, Entrust may invoice Customer the full costs of returning the Hardware.

9.3.4.2.3. Customer shall be responsible for the removal and return of the Hardware that has experienced a Problem and the installation of the replacement Hardware unless the Customer has purchased the *Rapid Delivery* option with respect to such Hardware. Failure to ship the original Hardware back to Entrust within a reasonable period of time following receipt of the replacement Hardware shall cause Customer to be responsible for the retail purchase of the replacement Hardware.

9.3.4.2.4. Reserved.

9.3.4.3. Hardware Upgrades.

Customer recognizes and acknowledges that as a replacement Hardware unit may contain a different or upgraded Software version or other product variants that have developed or evolved over time, a possibility exists that such replacement Hardware unit may not be immediately compatible with Customer's operating environment such as to require Customer to make adjustments to its operating environment.

9.4. **Reserved**.

9.4.1 .

9.5. **Customer Obligations**.

9.5.1. The Customer shall:

9.5.1.1. General.

9.5.1.1.1. Promptly report any identified Problem to Entrust by logging it into the Support Help Center or by email or by telephone as described in the Welcome Pack, documenting it in sufficient detail for Entrust to be able to recreate the Problem, in compliance with its information security responsibilities set forth below, and by providing: Hardware Serial number, a description of the Problem and the circumstances in which it occurred, information on the supported Hardware and/or Software, e.g. software version, license number, environment etc., diagnostic information (logs, debugs) and an assessment of the severity of the Problem in terms of operational impact;

9.5.1.1.2. Quote the Entrust contract number when reporting the initial problem. Once the Problem has been logged and assigned a ticket number, this number should be quoted in all further communications;

9.5.1.1.3. Use Hardware and/or Software in accordance with the Documentation and promptly and regularly carry out all operator maintenance routines as and where specified;

9.5.1.1.4. Use with Hardware operating supplies and media which comply with Entrust's recommendations;

9.5.1.1.5. Permit only Entrust or Entrust's approved agents to adjust, repair, modify, maintain or enhance the Hardware or Software, save for any operator maintenance specified for Hardware, in which case, permit the Hardware to be used or operated only by properly qualified operators directly under Customer's control;

9.5.1.1.6. Keep adequate back-up copies of the software, data, databases and application programs in accordance with best computing practice. Customer agrees that it is solely responsible for any and all restoration and reconstruction of lost or altered files, data and programs;

9.5.1.1.7. Maintain consistently the environmental conditions recommended by Entrust; and

9.5.1.1.8. Install and implement all solutions, corrections, resolutions, hot fixes and new releases in accordance with Entrust's installation instructions. Customer acknowledges that failure to install such solutions, corrections, resolutions, hot fixes and new releases may cause the Software to become unusable or non-conforming and may cause subsequent corrections and Updates to be unusable. Entrust accepts no liability for the performance of the Software that has not been installed in accordance with Entrust's installation instructions.

9.5.1.2. Access.

9.5.1.2.1. In the event that Entrust agrees to send an engineer to Customer's site, Customer shall permit reasonable access to the Hardware and/or Software for the purpose of carrying out the Support Services and shall make available suitable staff, telecommunications facilities and connections, modem links, electricity, light, heating and other normal services and operating time on any associated system to enable tests to be carried out, including at any remote location if necessary for this purpose. Customer shall provide the Entrust personnel access to the Hardware and/or Software in a place, which conforms to the health and safety regulations of the country where the Entrust personnel is to perform such Support Services.

9.5.1.2.2. Entrust will not require access to any Customer data other than basic contact information from select Customer representatives to provide Support Services and Customer shall take appropriate precautions to prevent transfer of any unnecessary Customer data to Entrust.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including, for example, training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligations and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate this Support Schedule immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate this Support Schedule in accordance with the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause.

Welcome to Entrust nShield as a Service Technical Support

Hardware and Supplies Schedule: March 2022

ENTRUST

Hardware and Supplies Schedule: March 2022

Contents

How to use Entrust nShield technical support services? 4
How to access the help center 5
How to subscribe to notifications and alerts 6
How to contact Entrust nShield technical support 7
What happens when you log a support ticket? 8
Anticipating our questions 9
How do we handle your ticket? 10
How to use Entrust nShield technical support services 11
Premium Plus 12

How to use Entrust nShield as a Service technical support services

Many questions and problems can be resolved using the online help center resources

How to contact us

There are three methods you can use to contact Entrust technical support to log a query:

1. Logging into the Entrust help center
2. Calling Entrust nShield technical support – (see the technical support section of this guide for contact information)
3. Emailing Entrust nShield technical support

The help center

The Entrust nShield technical support help center can be accessed from the following link: nshieldsupport.entrust.com

Gaining access to this site requires an active support contract

The Entrust nShield help center offers the following benefits:

- Available 24x7: The Entrust help center is an easy to use self-service portal that provides unlimited access to a wealth of information via the web 24x7
- Search the Entrust nShield knowledge base: Through our comprehensive search capability, the help center offers a knowledge base with valuable troubleshooting advice, how-to articles, and best practices
- Subscribe to product notifications and alerts: The Entrust help center offers a subscription feature that provides notifications of new software releases, product updates, security alerts, and other important support-related news

Once you have a registered account for the help center, to subscribe for updates, you simply select the product group you would like to be notified about.

Many questions and problems can be resolved using the help center resources such as product documentation, product release notes, security alerts, and bug information.

How to access the help center

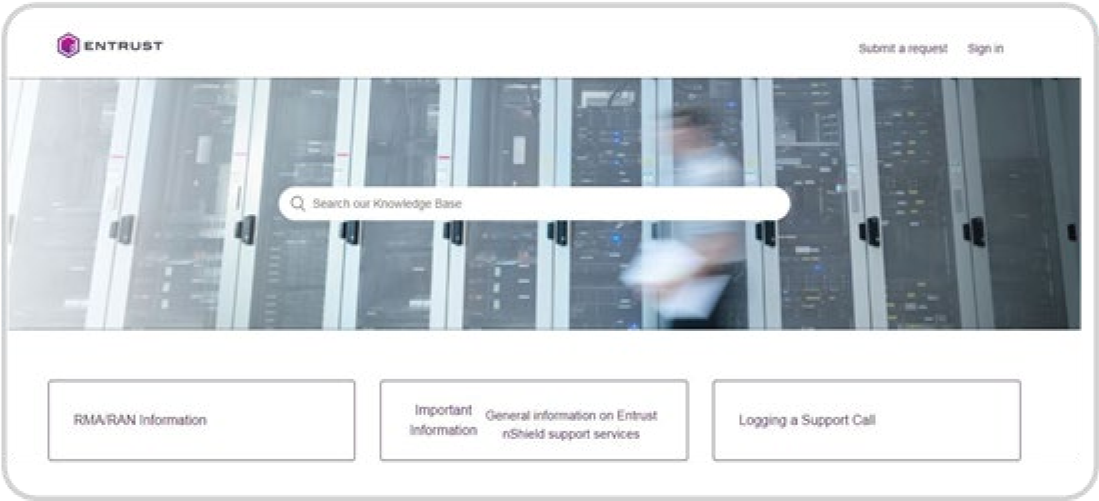
Request login credentials

Before you can access all of the help center articles or submit support requests you must have an account with Entrust.

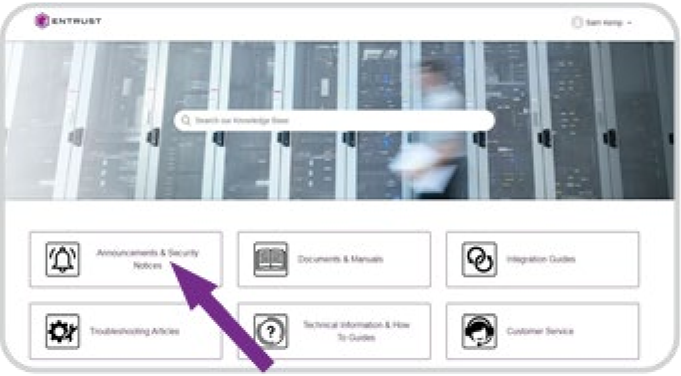
Anyone with a current valid support contract can get an account.

Either email the Entrust support team at nshield.support@entrust.com or phone using the contact numbers from the How to contact us section in this welcome pack.

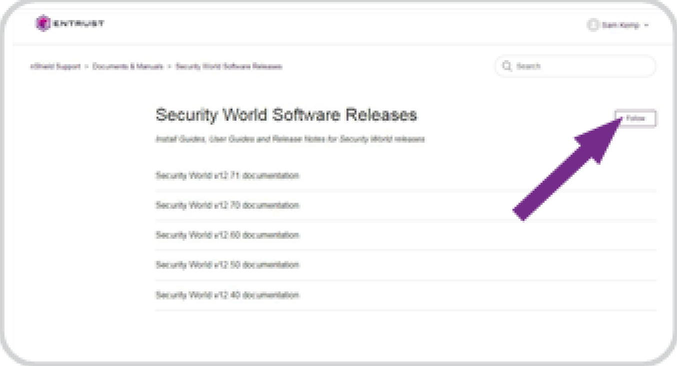
If you already have an account but don’t know your password, you can click the “forgot my password” link to reset your access to the site.



How to subscribe to notifications and alerts


ENTRUST
Sam Kemp
Search our Knowledge Base
Announcements & Security Notices
Documents & Manuals
Integration Guides
Troubleshooting Articles
Technical Information & How To Guides
Customer Service

1. Select the topic of interest


ENTRUST
Sam Kemp
nShield Support › Documents & Manuals › Security World Software Releases
Search
Follow

Security World Software Releases

Install Guides, User Guides and Release Notes for Security World releases

Security World v12.71 documentation

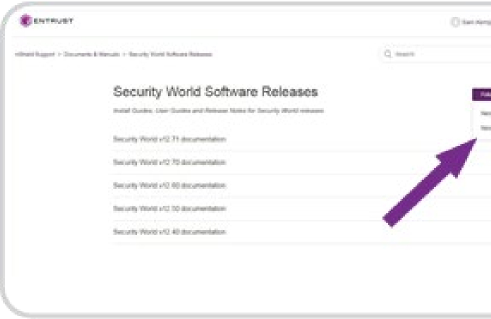
Security World v12.70 documentation

Security World v12.60 documentation

Security World v12.50 documentation

Security World v12.40 documentation

2. Click on "follow"



nShield Support > Documents & Manuals > Security World Software Releases

Security World Software Releases

Install Guides, User Guides and Release Notes for Security World releases

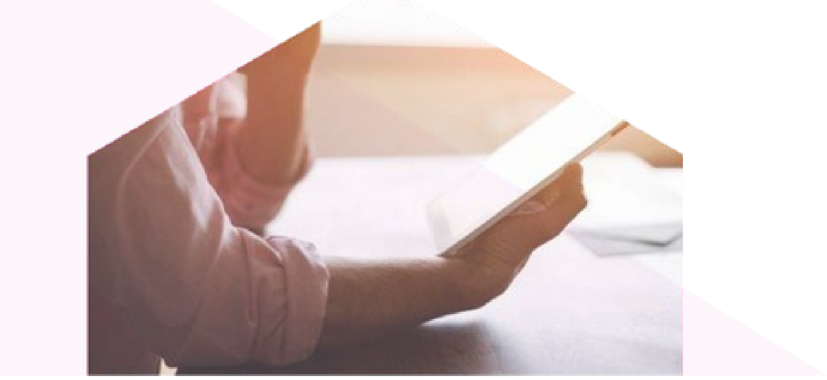
Security World v12.71 documentation

Security World v12.70 documentation

Security World v12.60 documentation

Security World v12.50 documentation

Security World v12.40 documentation



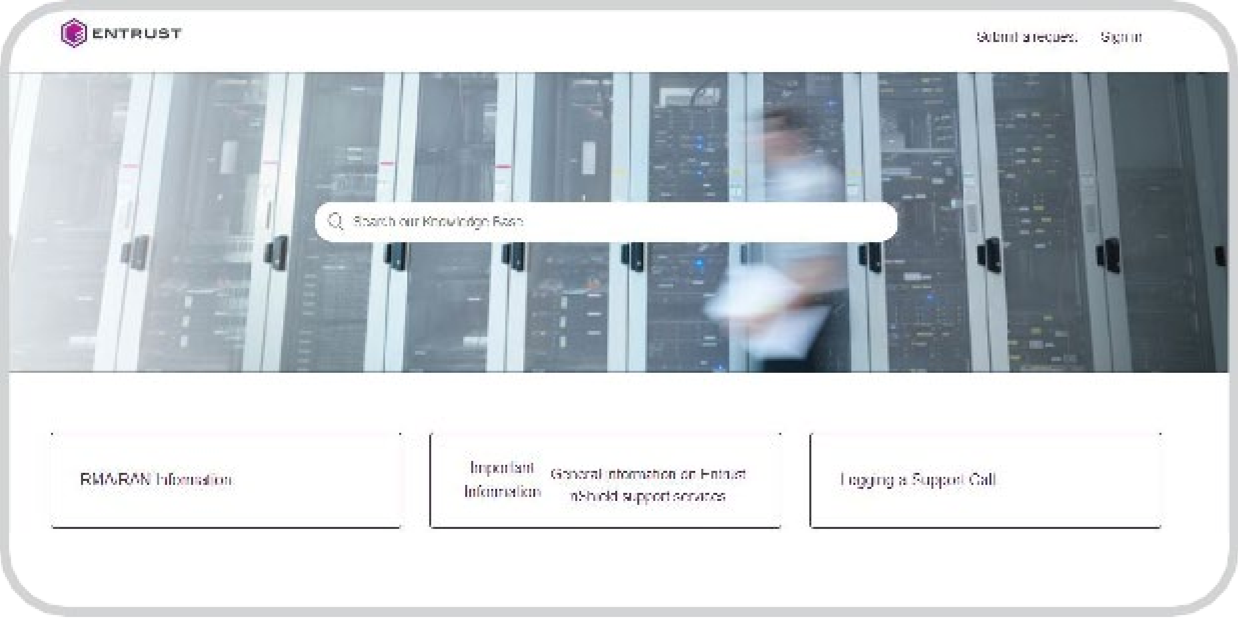
3.
Select the
“new articles” option

How to contact Entrust technical support

By the help center

You can raise a support ticket through our help center. Simply log in and click on the “submit a request” button in the top navigation menu. nshieldsupport.entrust.com

ENTRUST



When reporting a problem we strongly recommend that you provide as much information as possible so that our support engineers can quickly begin the troubleshooting process.

By email

If you wish to contact us by email, our email address is: nshield.support@entrust.com

When we receive your email a ticket will be logged and an Entrust support engineer will contact you within the targeted time of your support contract.

Email is monitored during normal business hours.

……………….By phone

You can also contact us by telephone, using the following numbers. PLEASE NOTE: Incoming and outgoing phone calls may be recorded for diagnostic, quality, and training purposes.

EMEA 8:30 am-5 pm (GMT)	**+44 1223 622444**

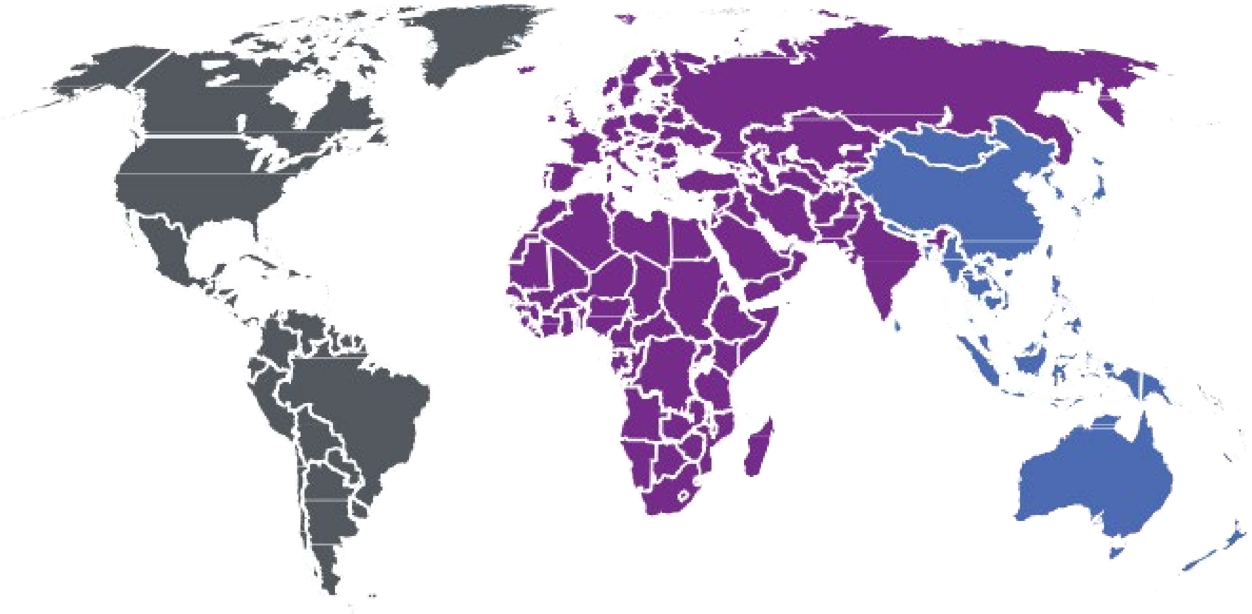
ENTRUST

APAC
9 am-5 pm (Hong
Kong) Australia
Japan

+852 3008 3188
+61 8 9126 9070
+81 50 3196 4994

AMERICAS
9 am-9 pm (GMT−5)
Brazil

+1 (833) 425-1990
+55 11 3230 5205



What happens when you log a support ticket?

✉ You will receive an email confirming your ticket reference number.

The ticket will be assigned to one of our knowledgeable technical support engineers, who will contact you to discuss the issue and plan the first steps toward reaching a resolution.

As the investigation into your issue progresses, we'll keep you updated on a regular basis. You can also check the current status

of the ticket via
our help center.

Anticipating our questions

We may need to ask you for some of the following information to help us find a resolution to your issue:

- Contract number or serial number
- A description of the fault and the circumstances in which it occurs
- Information on the supported software (if applicable) e.g., version, license number, environment, etc.
- Diagnostic information (e.g., logs/debug/trace files/core dumps)
- An assessment of the severity of the fault in terms of the operational impact on your organization (please refer to the table overleaf)

ENTRUST

How do we handle your ticket?

We prioritize the ticket based on the severity of the impact on your environment and the service level you have purchased. Please refer to the following table when logging a support ticket through the help center.

TICKET SEVERITY	DEFINITION	RESULT
Severity 1	**Urgent:** Severe problem preventing customer from performing critical business functions	1. Production system crash or hang 2. Production data corruption (data loss, data unavailable) 3. Production systems significantly impacted, such as severe performance degradation 4. Production system and/or data is at high risk of potential loss or interruption 5. Production system work-around is required immediately
Severity 2	**High:** Customer or workgroup able to perform job function, but performance of job function degraded or severely limited	1. Production system adversely impacted 2. Non-production data corruption (data loss, data unavailable) 3. Non-production system crash or hang 4. Non-production system and/or data are at high risk of potential loss or interruption 5. Non-production system work-around is required immediately 6. Development system(s) is inoperative
Severity 3	**Normal:** Customer or workgroup performance of job function is largely unaffected	1. Production or development system has encountered a non-critical problem or defect 2. Questions on product use

ENTRUST

Severity 4	**Low:** Minimal system impact; includes feature requests and other non-critical questions	Question/Request for Information/Administration Queries

✓

How to use Entrust nShield technical support services

Phone support 24 × 7 × 365	✓
Phone support during regional business hours*	✓
Log requests via help center and email support (regional business hours)	✓
Maximum 4 hour response to initial query	✓
Access to knowledge articles, product announcements, and information via help center	
Firmware and software updates	✓
Hot fix for firmware and software issues, if available	✓

*See section How to contact Entrust nShield technical support

Premium Plus

- 24/7 access to our expert technical support via web portal, phone,

and email

- Initial response within 4 hours
- Critical incident management process, to handle mission critical technical issues
- Hot fixes for software and firmware issues
- Access to the help center and knowledgebase
- Software, firmware, and documentation updates
- Priority escalation handling

Our Premium Plus support package provides our highest level of 24x7 technical support. It is designed for organizations who cannot allow their business to be impacted by extended outages within their critical live environment.

Premium Plus support includes access to our highly skilled team of technical support engineers, 24 hours a day, 365 days a year (by phone only at weekends and public holidays).

ENTRUST

For any non-critical changes required at the HSM, please log a ticket with Entrust nShield as a Service technical support. An initial response, confirming an estimated date for the change will be provided within 5 working days

To find out more about Entrust nShield HSMs

HSMinfo@entrust.com

entrust.com/HSM

ENTRUST

ABOUT ENTRUST CORPORATION

Entrust keeps the world moving safely by enabling trusted identities, payments and data protection. Today more than ever, people demand seamless, secure experiences, whether they're crossing borders, making a purchase, accessing e-government services, or logging into corporate networks. Entrust offers an unmatched breadth of digital security and credential issuance solutions at the very heart of all these interactions. With more than 2,500 colleagues, a network of global partners, and customers in over 150 countries, it's no wonder the world's most entrusted organizations trust us.

Learn more at

entrust.com

..................Column Break..................

ENTRUST

Global Headquarters
1187 Park Place, Minneapolis, MN 55379
U.S. Toll-Free Phone: 888 690 2424
International Phone: +1 952 933 1223

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope**.

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery**. Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty**.

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination**.

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users**. Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source.** Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Identity as a Service

Terms Of Service

The Agreement for Entrust's Identity as a Service Offering ("IDaaS") is made up of these terms of service (the "IDaaS Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for IDaaS. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity.

IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE OFFERING. THE CONTINUED RIGHT TO ACCESS AND USE THE OFFERING IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Definitions.** The following capitalized terms have the meanings set forth below whenever used in this IDaaS Schedule.

1.1. "Authentication Record" means a record setting out the details of each authentication attempt made by a User. Authentication Records may include Personal Data.

1.2. "AUP" means Entrust's acceptable use policy, as may be non-materially modified from time to time and attached hereto.

1.3. "Customer Account" means the account Customer sets up through the Hosted Service once Customer has agreed to the terms and conditions of the Agreement, including any subordinate accounts.

1.4. "Customer Data" means any data, or information that is supplied to Entrust (or its sub-processors) on Customer's behalf, through the Customer Account or otherwise in connection with Customer's or its Users' use of the Entrust Technology (including without limitation, device and computer information). Customer Data may include Personal Data, but excludes Service Data, Profile data, Customer Confidential Information and Excluded Data.

1.5. "Customer Systems" means computer systems or networks under the ownership, possession or control of Customer, for which the Hosted Service is being used to authenticate Users' access.

1.6. "Documentation" means written materials prepared by Entrust (or its licensors or service providers) relating to the Entrust Technology, including, without limitation, guides, manuals, instructions, policies, reference materials, professional services bundle descriptions, release notes, online help or tutorial files, support communications (including any disputes between the parties) or any other materials provided in connection with modifications, corrections, or enhancements to the Entrust Technology, all as may be modified from time to time.

1.7. "Entrust Technology" means the Hosted Service, the Software, the Tokens, and the Documentation.

1.8. "Extension" means an Entrust suite, configuration file, add-on, software integration, technical add-on, example module, command, function or application separately licensed by Entrust to Customer, that extends the features or functionality of third-party software or services separately licensed or lawfully accessed by Customer.

1.9. “Hosted Service” means, in this IDaaS Schedule, the Identity as a Service cloud-based platform which Entrust hosts on its (or its hosting providers’) computers.

1.10. “Professional Services” means professional services made available in relation to the Entrust Technology as described in Documentation, and that incorporate by reference the Professional Services Special Terms and Conditions. Professional Services shall not include Support Services.

1.11. “Profile” means User and device profiles constructed from authentication patterns and device-identifying technical data. Profiles may include data from third party service providers, and may also include Personal Data.

1.12. “Service Data” means any information and data relating to the access, use, and/or performance of the Entrust Technology, including data generated in connection with Customer’s and/or Users’ use of the Entrust Technology (e.g., analytics data, statistics data and performance data). Service Data does not include Authentication Records, Customer Data, Profiles, or Personal Data.

1.13. “SLA” means Entrust’s standard service level agreement for the Hosted Service, as may be non-materially modified from time to time, and attached hereto.

1.14. “Software” has the meaning set out in the General Terms, and in this IDaaS Schedule includes the Entrust Identity as a Service Gateway software application, and any updates, new versions, or replacement versions Entrust provides to Customer, as applicable.

1.15. “Special Terms and Conditions” means any terms and conditions attached to this IDaaS Schedule.

1.16. “Tokens” means the tokens (if any) specified in the Order.

1.17. “Third-Party Integrations” has the meaning set out in Section 5.9 (*Third-Party Integrations*).

1.18. “User” has the meaning set out in the General Terms, and in this IDaaS Schedule includes any individual end user who accesses or uses the Hosted Service through the Customer Account via the Hosted Service portal or otherwise (e.g. API-based access).

2. **Hosted Service; Software**.

2.1. Hosted Service. Customer receives no rights to the Hosted Service other than those specifically granted in Section 2.1 (Hosted Service).

2.1.1. Right to Access and Use. Subject to Customer’s compliance with the Agreement, Entrust grants Customer, during the Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Service: (i) via the Hosted Service portal or otherwise (ii) in accordance with the AUP; (iii) in accordance with the Documentation; (iv) in accordance with any specifications or limitations set out in the Order or imposed by technological means of the capabilities of the Hosted Service that Customer is permitted to use, such as limits associated with number of Users, or bundle entitlements, etc.; (v) for the sole purpose of authenticating the identity of Users; and (vi) subject to the general restrictions set out in Section 8 of the General Terms (*General Restrictions*).

2.1.2. Licenses from Customer. Customer grants to Entrust a non-exclusive, nontransferable worldwide right to copy, store, record, transmit, display, view, print or otherwise use any trademarks that Customer provides Entrust for the purpose of including them in Customer’s user interface of the Hosted Service (“Customer Trademarks”).

2.1.3. Service Levels. The sole remedies for any failure of the Hosted Service are listed in the SLA. Service credits issued pursuant to the SLA, if any, will only be applied against the costs associated with Customer’s subsequent subscription renewal. Entrust is not required to issue refunds for or to make payments against such service credits under any circumstances.

2.1.4. Service Revisions. Entrust may modify or eliminate Hosted Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to the Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice at the Hosted Service portal constitutes written notice). In the event that an Entrust change has a material detrimental impact on the Hosted Service that Customer has purchased, Customer may elect to terminate the affected Hosted Service and Customer shall be entitled to a pro rata refund for any fees pre-paid by Customer for the portion of the affected Hosted Service not yet provided or delivered by Entrust as of the date of termination. It will be Customer's responsibility to notify its Users of any such changes.

2.1.5. Users; Configuration and Security Measures. Customer is responsible and liable for any and all acts and/or omissions of its Users in relation to or breach of the Agreement or otherwise in relation to Users' access to and use of the Hosted Service. Customer will (i) only permit Users access to and use of the Hosted Service in combination with Customer's products or systems; (ii) prohibit any User from decompiling, reverse engineering or modifying the Hosted Service (except as and only to the extent any foregoing restriction is prohibited by applicable laws, rules, or regulations); (iii) make no representations or warranties regarding the Hosted Service to Users for or on behalf of Entrust; (iv) not create or purport to create any obligations or liabilities on or for Entrust regarding the Hosted Service. Customer is also responsible and liable for: (a) account usernames, passwords and access tokens; (b) the configuration of the Entrust Technology to meet its own and its Users' requirements; (c) Customer Data, Profiles, Personal Data, and any other data uploaded to the Hosted Service through the Customer Account or otherwise by Customer or its Users; (d) Customer's or its Users' access to and use of the Hosted Service; (e) any access to and use of the Hosted Service through the Customer Account; and (f) maintaining adequate security measures and the legally required protection for Customer Systems and data in Customer's possession or control or data otherwise residing on Customer Systems.

2.2. Software. Customer receives no rights to the Software other than those specifically granted in Section 2.2 (Software).

2.2.1. License. Subject to Customer's compliance with the Agreement, Entrust hereby grants Customer a personal, non-exclusive, non-transferable, non-sub-licensable license to download, install, and use the Software, in object code form only, for the sole purpose of conducting Customer's internal business operations, and not for resale or any other commercial purpose, all in accordance with: (i) the Documentation; and (ii) any specifications or limitations set out in the Order or imposed by technological means of the capabilities of the Software that Customer is permitted to use.

2.2.2. Licensed Not Sold. Copies of the Software provided to Customer pursuant to the Agreement are licensed, not sold, and Customer receives no title to or ownership of any copy of the Software itself. Furthermore, Customer receives no rights to the Software other than those specifically granted in Section 2.2.1 (*License*) above.

2.2.3. Hosting and Management. Customer agrees that it will be responsible for installing and managing the Software on its own premises in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Hosted Service resulting from Customer's improper installation and/or management of the Software.

2.3. Documentation. Customer may use the Documentation solely as necessary to support Customer's access to and use of the Entrust Technology. Each permitted copy of all or part of the Documentation must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust or downloaded or otherwise accessed by Customer.

2.4. Support. Entrust provides the support commitments set out in the Support Schedule attached hereto for the Hosted Service. The "Silver Support Plan", as described in the Support Schedule, is included at no additional charge with a subscription to the Hosted Service. Other levels of Support may be available for purchase for an additional fee.

2.5. Unauthorized Access. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Entrust Technology or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

3. Evaluation; NFR.

3.1. Evaluation Purposes. Entrust may grant Customer the right to download, install, access, and use the Entrust Technology for evaluation purposes for the Trial Period. During the Trial Period Customer may not (i) use the Entrust Technology in order for Customer to generate revenue; or (ii) use any Customer Data or Personal Data in its evaluation of the Entrust Technology - only fictitious non-production data can be used.

3.2. Not-for-Resale (NFR) Purposes. Entrust may grant Customer the right to download, install, access, and use the Entrust Technology for not-for-resale (NFR) purposes for the NFR Period. NFR rights are granted to Customers that are Entrust authorized distributors, resellers, or indirect resellers (for the purposes of this Section, "Authorized Resellers"). During the NFR Period Authorized Reseller may download, install, access, and use the Entrust Technology for purposes of development, testing, support, integration, proofs of concept and demonstrations. Customer shall not use any Customer Data or Personal Data in its NFR use of the Entrust Technology other than Customer Data or Personal Data that is from its own personnel (i.e. not that of prospective clients) or other third parties.

3.3. Inapplicable Sections. Section 2.1.3 (*Service Levels*) does not apply to Customer's download, installation, access, or use of the Entrust Technology for evaluation or NFR purposes.

3.4. Trial Period. Customer's evaluation of the Hosted Service pursuant to this Section 3 (*Evaluation; NFR*) shall commence upon Customer's acceptance of the Agreement and continue for a period of thirty (30) days ("Trial Period"), or as otherwise agreed to by Entrust in writing with Customer.

3.5. NFR Period. Customer's access to and use of the Entrust Technology for NFR purposes pursuant to this Section 3 (*Evaluation; NFR*) shall commence on Customer's acceptance of the Agreement and continue for the duration indicated in the Order or the Documentation ("NFR Period").

3.6. Termination or Suspension. Notwithstanding the foregoing, Entrust may in its sole discretion suspend or terminate Customer's evaluation or NFR access to and use of, the Entrust Technology at any time, for any or no reason, without advanced notice.

4. Fees. Customer will pay the costs and fees for the Entrust Technology as set out in the applicable Order in accordance with the GSA Schedule Pricelist, which are payable in accordance with the Order and the General Terms.

5. Data and Privacy.

5.1. Customer Data; Profiles; Authentication Records; Personal Data. Customer acknowledges and agrees that the Entrust Technology requires certain Customer Data, Profiles, and Personal Data, in order to operate. Use of the Entrust Technology by Customer and Users will also generate Authentication Records. Customer grants to Entrust, its Affiliates, and any of their respective applicable subcontractors and hosting providers, a world-wide, limited right, during the Term, to host, copy, store, transmit, display, view, print or otherwise use Customer Data and Personal Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers) to provide the Entrust Technology in accordance with the Agreement.

5.2. Service Regions. Customer will select the geographic region(s) (each a "Service Region") where Authentication Records, Customer Data, Profiles and Service Data will be stored (subject to any limitations of Entrust's hosting providers). With respect to the Authentication Records, Customer Data, Profiles and Service Data, and any Personal Data contained therein, that Entrust may collect hereunder, Customer consents to the storage in and/or the transfer into, the Service Region(s) which the Customer has selected. Notwithstanding the foregoing, Customer acknowledges and agrees: (i) that Entrust may send short message service (SMS) messages through the United States and/or Canada as part of the Entrust Technology; and (ii) Customer's billing information may be stored in the United States and/or Canada.

5.3. Profiles; Service Data; Use of Data. Entrust owns all right, title and interest in and to Service Data and Profiles (excluding any Personal Data contained in the Profiles) and, without limiting the generality of the foregoing, may use, reproduce, sell, publicize, or otherwise exploit such Profiles and Service Data in any way, in its sole discretion.

5.4. Consents. Customer represents and warrants that, before authorizing a User to use the Entrust Technology and before providing Customer Data or Personal Data to Entrust, Customer will have obtained from Users the requisite consents (if any) or satisfied other legal basis of processing Personal Data, and made all requisite disclosures (if any) to Users, in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data, by Entrust (including by any of its applicable subcontractors or hosting service providers) in accordance with the Agreement.

5.5. Consents Relating to Extensions. Customer acknowledges and agrees that certain Extensions may enable third-party software or third-party services (including cloud services) to download certain Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data from the Entrust Technology, and, by enabling such third-party software or third-party services (including cloud services) Customer agrees to such downloads. Customer represents and warrants that, before using any Extension, Customer will have obtained from Users the requisite consents (if any) or satisfied other legal basis of processing Personal Data, and made all requisite disclosures (if any) to Users, in accordance with all applicable laws, rules or regulations in order to allow for the downloading and/or transfer of such Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data, from Entrust (including any applicable subcontractors and hosting providers) to the Customer-licensed third-party software or third-party services (including cloud services) enabled by the Extension.

5.6. Consents Relating to Third-Party Service Providers. Customer consents to, and represents and warrants that it will obtain all Users' consents necessary for, Entrust's use of third-party service providers, including, without limitation, hosting providers (who may further utilize subcontractors) in the provision of the Hosted Service. Customer acknowledges and agrees that Authentication Records, Customer Data, Profiles, Personal Data, and Service Data, may be transmitted to, processed by and/or reside on computers operated by the Entrust authorized third parties (e.g. Entrust's hosting providers) who perform services for Entrust. These third parties may use or disclose such Authentication Records, Customer Data, Profiles, Personal Data, and Service Data to perform the Hosted Service on Entrust's behalf or comply with legal obligations. Unless otherwise required by applicable laws, rules or regulations, and without limiting the generality of Section 10 (*Liability*), Entrust shall have no responsibility or liability for Customer's failure to obtain any of the consents or disclosures described in this Section (*Consents Relating to Third-Party Service Providers*).

5.7. Third-Party Integrations. Customer may enable integrations between the Entrust Technology and certain third-party services contracted by Customer (each, a "Third-Party Integration"). By enabling a Third-Party Integration between the Entrust Technology and any such third-party services, Customer is expressly instructing Entrust to share all Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data, necessary to facilitate the Third-Party Integration. Customer is responsible for providing any and all instructions to such third part services provider about the use and protection of such Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data. Customer acknowledges and agrees that Entrust is not a sub-processor for any such third-party services providers in relation to any Personal Data contained in the aforementioned data or information, nor are any such third-party services providers sub-processors of Entrust in relation to any Personal Data contained in the aforementioned data or information.

5.8. Data Accuracy. Entrust will have no responsibility or liability for the accuracy of data uploaded to the Hosted Service by Customer or its Users, including, without limitation, Customer Data, Profiles, and Personal Data. Customer shall be solely responsible for the accuracy, quality, integrity, and legality of Customer Data or Personal Data and the means by which Customer acquired them.

6. Feedback.

6.1. Feedback. “Feedback” refers to Customer’s suggestions, comments, or other feedback about the Entrust Technology or other Entrust products and services. Even if designated as confidential, Feedback will not be subject to any confidentiality obligations binding Entrust. Customer hereby agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust all of Customer’s right, title, and interest thereto, including without limitation intellectual property rights. Entrust acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

7. Warranty Disclaimers.

7.1. Warranty Disclaimers. For the purposes of this IDaaS Schedule, the following is added to the disclaimer of warranties in the General Terms: Entrust makes no representations, conditions or warranties: (i) that the Entrust Technology will be free of harmful components; (ii) that Authentication Records, Customer Data, Profiles, Personal Data, and/or Service Data or any other Customer content or data stored in, transferred to or from, or otherwise processed by the Entrust Technology, including in transit, will not be damaged, stolen, accessed without authorization, compromised, altered, or lost.

8. Indemnities.

8.1. Reserved

9. Term, Termination and Suspension.

9.1. Term. The Hosted Service is sold on a subscription basis. Unless otherwise specified on the Order, the Offering Term for the Hosted Service will commence on the date that the Order is accepted by Entrust and will continue in effect for the period specified in the Order (or until the date the Trial Period or NFR Period expires), unless terminated in accordance with the Agreement.

9.2. Termination. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

9.3. Suspension by Entrust. Entrust may, at its sole discretion, temporarily suspend Customer’s or its Users’ access to the Entrust Technology at any time, without advanced notice, if: (i) reserved; (ii) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers’ or users’ information or data processed by the Entrust Technology; or (iii) Reserved. Entrust may also, without notice, suspend Customer’s or User’s access to the Entrust Technology for scheduled or emergency maintenance. Termination of the Agreement will result in termination of all Orders.

9.4. Effects of Termination. Without limiting the generality of the effects of termination set out in the General Terms, upon termination or expiration of the Hosted Service, Entrust will have no further obligation to provide the Entrust Technology, Customer will immediately cease all use of the Entrust Technology, and Customer will return all copies of Confidential Information to Discloser or certify, in writing, the destruction thereof, destroy any copies of Documentation, and delete any Software in its possession or control. Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Any provision of this Agreement which contemplates or requires performance after the termination of this Agreement or that must survive to fulfill its essential purpose, including the terms of this Section (*Effects of Termination*), confidentiality, disclaimers, limitations and exclusions of liability, and any payment obligations, will survive the termination and continue in full force and effect until completely performed. Termination or expiration (non-renewal) of the Agreement also terminates all Special Terms and Conditions and the parties’ ability to enter into any new Orders (including Orders to renew). Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Termination will not relieve Customer (directly or through an authorized reseller) from any obligation to pay Entrust any and all fees or other amounts due under the Agreement.

10. Miscellaneous.

10.1. Order of Precedence. In the event of a conflict or differences between this IDaaS Schedule and Special Terms and Conditions, the Special Terms and Conditions will prevail over any conflicting provisions.

10.2. Publicity. During the Term and for thirty (30) days thereafter, Customer grants Entrust the right, free of charge, to use Customer's name, worldwide, to identify Customer as such on Entrust's website or other marketing or advertising materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

10.3. Extensions and Third-Party Integrations. Customer's use of any Extension shall be subject to a separate end user license agreement (or other applicable agreement) between Customer and Entrust (or one of its Affiliates). Customer's use of any Third-Party Integration shall be subject to the separate end user license agreement (or other applicable agreement) between Customer with the relevant third party (e.g. service provider that provides the service which is the subject of the Third-Party Integration).

10.4. Tokens. If an Order calls for Tokens (or if Customer purchases Tokens through an Authorized Reseller), (i) Customer will be the importer of record and responsible for all freight, packing, insurance and other shipping-related expenses; (ii) risk of loss and title to the Tokens will pass to Customer upon delivery of the Tokens by Entrust (or an Authorized Reseller) or one of their respective agents to the carrier; (iii) the Tokens will be free from material defects in materials and workmanship and will conform to the published specifications for such Tokens in effect as of the date of manufacture for a period of one (1) year from the date on which such Tokens are first delivered to Customer (or for such extended warranty period as may be set out in the applicable Order); (iv) Customer will use Entrust as Customer's point of contact for Token warranty inquiries; and (v) as an express condition of the sale, Customer acknowledges that Customer is only permitted to use Tokens with the Hosted Service and Customer is expressly prohibited from using and agrees not to use Tokens with any other provider's verification or identification software even if the Tokens may interoperate with such other provider's verification or identification software. The aforementioned Token warranty will not apply where the issue is caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Token. Any Token that is replaced becomes the property of Entrust. Entrust's exclusive liability and Customer's exclusive remedy for breach of this Section (*Tokens*) is for Entrust, at its option, to repair or replace the Token, or take return of the Token and refund the price paid for the Token.

10.5. Customer Using Hosted Service Provider Functionality for its Affiliates. Where Entrust enables and Customer chooses to utilize the "service provider" functionality in respect of Customer Affiliates, (i) Customer will be permitted to allocate the aggregate number of User entitlements set out on the Order between Customer and its Affiliates, and (ii) each of Customer's Affiliates to which subscriptions are allocated will be deemed to be the Customer for purposes of the Agreement and bound by the terms and conditions of the Agreement as if such Affiliate was Customer itself. Customer agrees to be jointly and severely liable for the performance (or non-performance) of the Agreement by each such Affiliate including, without limitation, any breach of the Agreement, any and all indemnification obligations contained within the Agreement, and any and all acts or omissions of each such Affiliate as if such actions or omission has been performed by Customer itself. Customer will provide Entrust with prior written notice before adding any Affiliate. Such notice will include each Affiliate's full corporate name and address as well a point of contact within the Affiliate. To the extent Entrust requires additional information about an Affiliate or their usage of the Hosted Service including, without limitation, as part of a lawful access request or subpoena, Customer will make best efforts in co-operating with Entrust. Customer will remain responsible for payment for all fees set out on its Order.

10.6. U.S. Government End-Users. The Software and Documentation are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If the Software and Documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to the Software and Documentation are limited to the commercial rights and restrictions specifically granted in the Agreement. The rights limited by the preceding sentence include, without limitation, any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the Software and Documentation. This Section (*U.S. Government End-Users*) does not grant

Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any legal notice appearing in the Software or Documentation or on any packaging or other media associated with the Software or Documentation.

10.7. Compliance with Applicable Laws. In addition to Customer's compliance obligations in the General Terms, Customer is responsible for ensuring that its use of the Entrust Technology, any Extensions, and any Third Party Integrations, complies with, and Customer will comply with its obligations under all applicable laws, rules or regulations, including, without limitation, all applicable privacy and data protection laws, rules or regulations governing the protection and transfer of Authentication Records, Customer Data and Profiles (including all Personal Data contained therein), and/or Service Data.

10.8. Amendment. This IDaaS Schedule may be non-materially amended by Entrust from time to time by posting a new version on its website, and such new version will become effective on the date it is posted except that if Entrust modifies this IDaaS Schedule in a manner which materially reduces Customer's rights or increases Customer's obligations and such changes are not required for Entrust to comply with applicable laws, the changes must be agreed by both parties in writing. If Customer objects in writing during that sixty (60) day period, the non-material changes to this IDaaS Schedule will become effective at the end of Customer's current subscription term. Notwithstanding the foregoing, provisions of this Section (*Amendment*), amendment of the AUP is governed by the AUP. This IDaaS Schedule may not be modified by Customer except by formal agreement in writing executed by both parties.

10.9. Insurance. Customer shall have and maintain in force appropriate insurance with reputable authorized insurers of good financial standing which shall cover the liability of Customer for the performance of its obligations under the Agreement. Customer shall provide to Entrust, upon written request from Entrust but not more than once in any twelve (12) month period, written confirmation from the arranging insurance brokers that such insurances are in effect. The provisions of any insurance or the amount of coverage shall not relieve Customer of any liability under the Agreement. It shall be the responsibility of Customer to determine the amount of insurance coverage that will be adequate to enable Customer to satisfy any liability in relation to the performance of its obligations under the Agreement.

Identity Proofing Special Terms and Conditions

These Identity Proofing Special Terms and Conditions ("ID Proofing Special Terms") are attached to the IDaaS Schedule, and contain the terms and conditions that govern access to and use of Identity Proofing (as defined herein). Capitalized terms not defined in Section 1 herein or elsewhere in these ID Proofing Special Terms shall have the meaning set out in the IDaaS Schedule. References to articles or sections herein shall be to articles or sections in these ID Proofing Special Terms unless otherwise expressly stated. Provisions in these ID Proofing Special Terms will prevail with respect to Identity Proofing over any conflicting provision in the IDaaS Schedule.

1. DEFINITIONS.

1.1. "Customer Application" means the application developed by Customer pursuant to the SDK License (as defined herein) to be used to access and use Identity Proofing.

1.2. "Customer Data", in addition to its meaning in the IDaaS Schedule, with respect to Identity Proofing means Device Information, Risk Information, Identity Proofing Results, as well as data or information collected using the Customer Application.

1.3. "Database" means the centralized Global Intelligence Platform owned, operated and maintained by Entrust (or its service providers) which contains Device Information and associated information including Risk information.

1.4. "Device" means a particular computer, mobile phone, desktop, tablet or other computing device.

1.5. "Device Information" means a set of Device attributes and characteristics that are designed to identify a particular Device.

1.6. "Identity Proofing" means the identity proofing functionality which forms part of the Hosted Service (if such functionality is selected by Customer and approved by Entrust in an Order).

1.7. "Identity Proofing SLA" means the Entrust's service level agreement specific to Identity Proofing, as set out in Attachment A to these ID Proofing Special Terms.

1.8. "Response" means the recommendation, including Risk Information, returned by Identity Proofing about a Device which has been evaluated by Identity Proofing.

1.9. "Risk" means risk including, without limitation, transaction, abuse, reputation and fraud risk.

1.10. "Risk Information" means information relating to specific Risk(s).

1.11. "SDK License" means the Entrust Mobile ID Proofing SDK License through which Customer may obtain a license to use the Mobile ID Proofing software development toolkit. The SDK License is not a part of the Agreement.

1.12. "User" has the meaning set out in the General Terms, and in these ID Proofing Special Terms includes any individual end user who accesses and/or uses Identity Proofing through the Customer Account, via the Customer Application.

2. USE OF IDENTITY PROOFING.

2.1. Grant of License. Subject to Customer's compliance with the Agreement, Entrust grants to Customer, during the ID Proofing Term (as defined herein), a worldwide, non-exclusive, nontransferable, non-sub-licensable right to, all in accordance with the Documentation, provide its User(s) with access to and/or use of Identity Proofing, through the Customer Account, via the Customer Application:

2.1.1. for the purpose of authenticating the identity of a User, extracting identity information or data from the User's identity document(s), and sending authentication results (resulting from (i) through (iv) above) to Customer

("Identity Proofing Results"), and not for resale or any other commercial purpose;

2.1.2. for the purpose of collecting and processing Device Information and providing Responses to Customer.

2.2. Restrictions. Identity Proofing shall not be available: (i) to MSPs or Tenants (as such terms are defined in the Managed Security Service Provider Special Terms and Conditions); and/or (ii) for not-for-resale (NFR) purposes.

2.3. Service Levels. The sole remedies for any failure of Identity Proofing are listed in the Identity Proofing SLA. Service credits issued pursuant to the Identity Proofing SLA, if any, will only be applied against the costs associated with Customer's subsequent subscription renewal. Entrust is not required to issue refunds for or to make payments against such service credits under any circumstances.

3. CUSTOMER DATA & PRIVACY.

3.1. Service Regions. The Service Regions available for selection by Customer may be different for Identity Proofing than for the main components of the Hosted Service, depending on the nature of the Customer Data, Personal Data, or Service Data (and the related Entrust hosting provider). With respect to the Customer Data and Personal Data that Entrust may collect pursuant to Identity Proofing, Customer consents to the storage in and/or the transfer into, the Service Region(s) which the Customer has selected. Customer further grants to Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers), a world-wide, limited right, during the ID Proofing Term, to host, copy, transmit and display Customer Data and Personal Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers) to provide Identity Proofing in accordance with the Agreement.

3.2. Excluded Data (Exception). Notwithstanding the provisions set out in Section 12.2 of the General Terms, Identity Proofing may involve the processing of Excluded Data. As such, Section 12.2 of the General Terms shall not apply with respect to any Excluded Data that is necessary or required in order for Entrust to provide Identity Proofing to Customer and its Users pursuant to the Agreement, but only to the extent necessary or required. Customer acknowledges and agrees that the provisions of Section 12.2 of the General Terms shall continue to apply in all other cases, along with all other disclaimers, limitations and exclusions contained in the IDaaS Schedule.

3.3. Consents; Accuracy; Rights. Customer represents and warrants that, before authorizing a User to use Identity Proofing and before providing Customer Data or Personal Data to Entrust, Customer will have provided and/or obtained the requisite rights, consents or permissions, and made all requisite disclosures (if any), to Users in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data contained therein, by Entrust (including any of its Affiliates, and any of their respective applicable subcontractors and hosting providers) in accordance with the Agreement. Customer further represents and warrants to Entrust that such Customer Data or Personal Data is accurate and up-to-date (and that Customer shall correct or update it as required), and that no Customer Data or Personal Data will violate or infringe (i) any third-party intellectual property, publicity, privacy or other rights; (ii) any applicable laws, rules or regulations or the AUP; or (iii) any third-party products or services terms and conditions. Customer will be fully responsible for any Customer Data or Personal Data submitted, uploaded, or otherwise provided to Identity Proofing by any User as if it was submitted, uploaded, or otherwise provided by Customer. Customer is solely responsible for the accuracy, content and legality of all Customer Data and Personal Data.

3.4. Rights in Customer Data and Personal Data. As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data and Personal Data provided to Entrust. Subject to the terms of the Agreement, Customer hereby grants to Entrust a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data and Personal Data contained therein solely to the extent necessary to provide Identity Proofing to Customer, and to sub-license such rights to any of Entrust's applicable subcontractors.

3.5. Rights in Certain Data (Device Reputation). As between the parties, Entrust owns and will retain all right, title and interest (including but not limited to any copyright, patent, trade secret, trademark or other proprietary and/or intellectual property rights) in and to Identity Proofing, and the Device Information, Database, and any Response.

For clarity, the foregoing does not mean that Entrust owns or retains any right, title or interest in or to the data elements comprising the Device Information, the Database, or any Response. The foregoing is an acknowledgement that, as between the parties, Entrust will retain any right, title and interest it may have in the Device Information, Database, and any Response, as collective works. Customer acknowledges that the Device Information and the Database, as collective works, may be Confidential Information of Entrust.

4. **CUSTOMER'S RESPONSIBILITIES, RESTRICTIONS & ACKNOWLEDGEMENTS**.

4.1. Compliance with Laws. Customer represents, warrants and covenants that is shall (i) use commercially reasonable efforts to prevent unauthorized access to, or use of, Identity Proofing and shall notify Entrust as soon as possible if it becomes aware of any unauthorized access or use of Identity Proofing; (ii) use Identity Proofing only for lawful purposes; (iii) not knowingly violate any law, rules or regulations of any country with its use of Identity Proofing; and (iv) not knowingly violate the intellectual property rights of any third party with its use of Identity Proofing.

4.2. Users; Identity Proofing Access. . Customer is responsible and liable for: (a) handling, use, and/or consequences or impact of Results or Responses resulting from use of Identity Proofing (e.g. impact on User's credit rating or ability to open accounts or any other unfavorable impact).

5. **TERM, TERMINATION & SUSPENSION**.

5.1. Term. Unless otherwise specified in the Order that includes the subscription for Identity Proofing, these ID Proofing Special Terms will commence on the date the Order is accepted by Entrust, and will remain effective for the subscription period specified for Identity Proofing in the Order, unless terminated earlier in accordance with the Agreement ("ID Proofing Term"). Upon expiration of the ID Proofing Term, Customer may elect to renew its subscription pursuant to these ID Proofing Special Terms for an additional length of time, as set forth in an Order for renewal, in which case the ID Proofing Term for Identity Proofing will be extended to include such additional length of time upon payment of the applicable fees for the additional length of time, all as set out in the Order for renewal.

5.2. Termination or Suspension for Cause. Entrust may, at its sole discretion, temporarily suspend Customer's and/or Users' access to Identity Proofing at any time, without advanced notice, if: (a) Entrust reasonably concludes that Customer and/or Users have conducted themselves in a way (i) that is not consistent with or violates the requirements of the AUP, the Documentation, or is otherwise in breach of the Agreement; or (ii) in a way that subjects Entrust to potential liability or interferes with the use of Identity Proofing by other Entrust customers and/or users; (b) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers' and/or users' information or data processed by Identity Proofing; or (c) Entrust reasonably concludes that Customer and/or Users are violating applicable laws, rules or regulations. Entrust may also, without notice, suspend Customer's and/or User's access to Identity Proofing for scheduled or emergency maintenance. Termination of these ID Proofing Special Terms will not necessarily result in termination of the entire Agreement (e.g. if Customer has an Identity as a Service subscription then the IDaaS Schedule and the applicable Order may still be active).

5.3. Effects of Termination. Upon termination or expiration of these ID Proofing Special Terms, Entrust will have no further obligation to provide Identity Proofing to Customer, Customer will immediately cease all use of Identity Proofing, and Customer will return all copies of Confidential Information to Entrust or certify, in writing, the destruction thereof, destroy any copies of Customer Data, Personal Data, Service Data, and Documentation (unless continued rights to use exist pursuant to the Agreement (e.g. if Customer continues to have an Identity as a Service subscription despite the termination or expiry to these ID Proofing Special Terms). Termination is without prejudice to any right or remedy that may have accrued or be accruing to either party prior to termination. Any provision of this Agreement which contemplates or requires performance after the termination of this Agreement or that must survive to fulfill its essential purpose, including the terms of this Section (*Effects of Termination*), confidentiality, disclaimers, limitations and exclusions of liability, and any payment obligations, will survive the termination and continue in full force and effect until completely performed.

Attachment A

To Identity Proofing Special Terms and Conditions

Identity Proofing SLA

Service Commitment
Entrust will use commercially reasonable efforts to make Identity Proofing available 99.8% of the time during any monthly billing cycle. In the event Identity Proofing does not meet the 99.8% target, Customer will be eligible to receive a Service Credit as described below.

Definitions. Capitalized terms not defined in this Attachment A shall have the meaning set out in the ID Proofing Special Terms.

- "**Monthly Uptime Percentage**" is calculated by subtracting from 100% the percentage of minutes during the month in which Identity Proofing was unavailable. Monthly Uptime Percentage measurements exclude downtime resulting directly or indirectly from any Exclusion (as defined below).

- "**Service Credit**" is, for the purposes of this Attachment A, a dollar credit, calculated as set forth below, that will be credited by Entrust to Customer's future invoices.

Service Credits
Service Credits are calculated based on the number of transactions that could have been processed during the downtime x the transaction fee that would have been paid by Customer if those transactions had been processed.

If the downtime is less than a full hour:
Step 1 – Calculate the Number of Transactions Processed During the Previous Calendar Quarter. The number of transactions that could have been processed is calculated based on the total number of transactions actually processed by Entrust on Customer's behalf during the calendar quarter immediately preceding the date on which the downtime occurred.

Step 2 – Calculate the Total Number of Hours in the Calendar Quarter. Calculate the number of days in the calendar quarter and multiply by 24 hours per day.

Step 3 – Divide Step 1 by Step 2 to arrive at the average number of transactions processed per hour during the previous calendar quarter:

$$\frac{\text{Step 1}}{\text{Step 2}} = \text{Average Number of Transactions Processed Per Hour}$$

Step 4 – Divide the amount of actual downtime by 60 minutes to arrive at the pro rata amount of an hour that the downtime represents:

$$\frac{\text{Minutes of Downtime}}{60} = \text{Pro Rata Portion of 1 Hour Represented by the Downtime}$$

Step 5 – Multiply the result of Step 4 (the pro rata portion of 1 hour represented by the downtime) by the result of Step 3 (the average number of transactions processed per hour) to arrive at the number of transactions that could have been processed during the downtime:

Step 4 x Step 3 = the Number of Transactions that Could Have Been Processed During the Downtime

Step 6 – Multiply Step 5 by the appropriate fee set forth in the applicable Order.

Step 5 x Transaction Fee = Service Credit

A Service Credit will be issued for the amount arrived at in Step 6.

If the downtime is a full hour:
For any full hour of unavailability, the Customer will receive a Service Credit for the number of transactions that could have been processed in the hour (Step 3) multiplied by the Transaction Fee set forth in the applicable Order.

Example:

- **Step 1** = 5,000 transactions during the previous calendar quarter
- **Step 2** = 91 days in the calendar quarter x 24 hour/day = 2,184 hours during the quarter
- **Step 3** = 5,000 (Step 1) divided by 2,184 (Step 2) = 2.5 transactions processed per hour
- **Step 4** = Assume downtime = 65 minutes so 60 minutes is one full hour leaving 5 minutes for the balance of the calculation. Divide 5 minutes by 60 minutes = 8.3% of an hour is represented by the downtime
- **Step 5** = 8.3% (Step 4) x 2.5 transactions processed during an hour (Step 3) = 1 transaction when rounded up to a whole transaction
- **Step 6** = 1 (Step 5) x $1.00 (transaction fee per transaction) = Service Credit of $1.00
- **Step 7** = Service Credit for less than a full hour (Step 6) + average number of transactions processed per hour (Step 3) multiplied by the transaction fee per transaction or $1 transaction fee + (2.5 average hourly transactions x $1 transaction fee) = $3.5 Service Credit for 65 minutes of downtime

Credit Request and Payment Procedures
Within thirty (30) days of the end of the relevant calendar month, Customer must submit a written request to Entrust for a Service Credit, along with sufficient information for Entrust to verify the time(s) and date(s) of the event for which Customer is claiming a Service Credit. If the Monthly Uptime Percentage when calculated by Entrust falls below the Uptime Guarantee, then Entrust will notify Customer that a Service Credit will be issued to Customer within one billing cycle following the month in which such request was confirmed by Entrust and the amount of the Service Credit. Customer's failure to request a Service Credit in a timely manner or provide sufficient information to Entrust that Entrust may reasonably request in order to verify the Monthly Uptime Percentage will disqualify Customer from receiving a Service Credit.

Exclusions
Exclusions shall not be included in the calculation of the time Identity Proofing was available in any given calendar month. As used herein, "Exclusion" shall mean any unavailability: (i) due to Entrust's planned maintenance or downtime the occurrence of which Customer received at least 24-hour advance written notice; (ii) caused by factors outside of Entrust's reasonable control, including any force majeure event or Internet access or related problems beyond the demarcation point of Identity Proofing; (iii) that result from the Customer Application, or failure of equipment, software, technology or facilities provided by Customer, including but not limited to, network unavailability or bandwidth limitations outside of Entrust's network; (iv) that results from a failure of the device reputation functionality made available as part of Identity Proofing; or (v) arising from Entrust's suspension and termination of Customer's right to use Identity Proofing in accordance with the Agreement.

Professional Services Special Terms and Conditions

These Professional Services Special Terms and Conditions ("PS Special Terms") are attached to the Entrust Identity as a Service IDaaS Schedule ("IDaaS Schedule") and contain the terms and conditions applicable for Professional Services. Capitalized terms not defined in Section 1 herein or elsewhere in these PS Special Terms shall have the meaning set out in the IDaaS Schedule. References to articles or sections herein shall be to articles or sections in these PS Special Terms unless otherwise expressly stated. Provisions in these PS Special Terms will prevail with respect to Professional Services over any conflicting provision in the IDaaS Schedule.

1. **DEFINITIONS**.

1.1. "Background IPR" means any intellectual property rights of a party or its Affiliates conceived, created, developed, or reduced to practice prior to, or independently of, the Professional Services provided under these PS Special Terms.

1.2. "Foreground IPR" means any intellectual property rights conceived, created, developed or reduced to practice by Entrust in the course of providing the Professional Services under these PS Special Terms.

2. **PROFESSIONAL SERVICES**.

2.1. Subject to Customer's compliance with the Agreement, Entrust shall perform the Professional Services for Customer as further described in an Order and any related Documentation.

2.2. Customer shall make available to Entrust any equipment, material, information, data and remote access as Entrust may reasonably require to perform the Professional Services.

2.3. Customer shall also provide Entrust with timely access to appropriate members of the Customer's staff as may be reasonably required by Entrust for the provision of the Professional Services (e.g. answering technical questions, other general questions as they may arise, and availability for meetings). Customer shall be responsible for the timely performance of its obligations under these PS Special Terms with respect to the requirements of Entrust in accordance with these PS Special Terms. Customer acknowledges that any delay on its part in the performance of its obligations may affect or delay Entrust's provision of the Professional Services.

2.4. Professional Services will be delivered remotely during Entrust regular business hours. No visits to Customer premises are included within the Professional Services, and no travel is required by or included within the Professional Services. Customer must provide Entrust remote access to systems as required for delivery of the Professional Services.

2.5. Each party shall designate a primary point of contact for matters relating to the Professional Services.

2.6. Out-of-Scope. Professional Services shall not include the following, which shall be Customer's responsibility: (i) initial setup (licensing, installation/deployment, configuration, verification) of the underlying non-Entrust infrastructure, including, without limitation, hardware, soft tokens, hard tokens, operating system (OS), software, client or virtual machines (VM); (ii) network, database, repository connectivity; (iii) configuration of network, firewall, load balancer, server or repository; (iv) configuration of third-party applications which will integrate with Entrust applications, other than where explicitly stated within the definition of the Professional Services; (v) any required Entrust software, seed files, and licenses

2.7. Warranty. Entrust represents to the Customer that the Professional Services performed pursuant to these PS Special Terms shall be performed in a professional manner in keeping with reasonable industry practices.

2.8. Non-Solicitation. Customer agrees that, without the prior written approval of Entrust, neither it nor its Affiliates will offer employment to any employees of Entrust nor will it directly or indirectly induce such employees to terminate their employment with their employer. This section is enforceable throughout the term of these PS Special Terms and shall survive for one (1) year following its termination for any reason.

3. **INTELLECTUAL PROPERTY**.

3.1. The Professional Services provided by Entrust pursuant to this Agreement are not “works for hire”.

3.2. The Background IPR of a party or its Affiliate shall remain the exclusive property of such party or its Affiliate and shall be deemed to be the Confidential Information of such party.

3.3. All right, title and interest in, to and under the Foreground IPR embodied in the Professional Services shall vest in and be owned by Entrust and shall be deemed to be the Confidential Information of Entrust.

3.4. In respect to the Foreground IPR and any Background IPR of Entrust (and its Affiliates) incorporated in a deliverable provided during the performance of the Professional Services, the Customer and its Affiliates are hereby granted a non-exclusive, non-transferable, royalty-free, worldwide, perpetual license to make, have made, use, copy and disclose such Foreground IPR and Background IPR, but solely to the extent necessary to use and exploit the deliverables provided during the performance of the Professional Services and only so long as such Foreground IPR and Background IPR is embedded in the deliverables and not separated therefrom. Any third party which receives such Foreground IPR and Background IPR shall be advised by the Customer in writing at the time of or before such disclosure, that proprietary confidential information is being communicated and that such information is to be kept confidential and not used except as permitted, and provided further, such third party undertake, in writing, prior to any such disclosure, to respect such obligations of confidence.

3.5. In respect to any Background IPR of the Customer and its Affiliates disclosed to Entrust and/or its Affiliates, Entrust and its Affiliates are hereby granted a non-exclusive, non-transferable, royalty-free, worldwide license for the term of this Agreement to make, use and copy such Background IPR, but solely to the extent necessary to provide the Professional Services to the Customer pursuant to these PS Special Terms.

3.6. Except as explicitly provided herein, no other license is granted under any intellectual property rights.

3.7. Nothing in these PS Special Terms shall prevent Entrust or its Affiliates from providing to a third party the same or similar professional services as those provided to the Customer pursuant to these PS Special Terms. The foregoing is subject to Entrust not breaching any of Customer’s proprietary rights.

ENTRUST IDENTITY AS A SERVICE ACCEPTABLE USE POLICY

This Acceptable Use Policy ("**AUP**") describes actions that Entrust prohibits when any party uses the Entrust Identity as a Service cloud-based authentication platform (the "**Service**"). The examples described in this AUP are not exhaustive. This AUP is incorporated by reference into, and governed by the Entrust Identity as a Service Schedule or other similar written agreement between you (individually and collectively the "Customer", "MSP", and/or "Tenant", hereinafter referred to as "**You**" and "**Your**") and the Entrust entity with which You entered into such agreement (the "**Agreement**"). References to "Entrust" shall also include, in addition to the Entrust contracting entity, its affiliates, subsidiaries, licensors, and other service providers. The Agreement contains definitions of capitalized terms not otherwise defined in this AUP (e.g. "Service", "Customer", "MSP", "Tenant", and "Agreement") and such definitions shall apply in this AUP (unless otherwise specified). The Agreement takes precedence over any conflicting provisions in this AUP. Entrust may modify this AUP at any time. Entrust will take commercially reasonable efforts to provide You with written notice (email or posting notice at the Service portal to suffice as adequate notice). By using the Service, You agree to the latest version of this AUP. If You violate the AUP or authorize, encourage or help others (including any of Your Users) to do so, we may suspend or terminate Your use of the Service (including that of any of Your Users).

Thus, You agree not to use, and not to encourage or allow any end user (including without limitation Users) to use, the Service in the following prohibited ways.

No Illegal, Harmful, or Offensive Use or Content

You may not use, or encourage, promote, facilitate or instruct others (i) to use the Service for any illegal, harmful, fraudulent, infringing, abusive or offensive use, or for any other activities that materially interfere with the business or activities of Entrust; or (ii) to transmit, store, display, distribute or otherwise make available content that is illegal, harmful, fraudulent, infringing or offensive. Prohibited activities or content include, without limitation:

- **Illegal, Harmful or Fraudulent Activities**. Any activities that: (i) are illegal, that violate the rights of others, or that may be harmful to others, Entrust operations or reputation, including disseminating, promoting or facilitating child pornography, offering or disseminating fraudulent goods, services, schemes, or promotions, make-money-fast schemes, ponzi and pyramid schemes, phishing, or pharming; (ii) violate or facilitate the violation of any local, state, provincial, federal, or foreign law or regulation, including, but not limited to, laws and regulations regarding the transmission of data or software and recording of phone calls and communications; (iii) use the Service in any manner that materially violates telecommunications industry standards, policies and applicable guidelines published by generally recognized industry associations, including those specifically communicated in writing to You by Entrust; (iv) use the Service to harvest or otherwise collect information about individuals, including email addresses or phone numbers, without their explicit consent or under false pretenses; (v) violate the privacy or data protection rights of any person (e.g. collecting or disclosing any information about an identified or identifiable individual protected under the privacy and/or data protection legislation applicable in the individual's jurisdiction without written permission); constitute cooperation in or facilitation of identity theft; (vi) degrade or negatively influence the good will or reputation of Entrust or that of its affiliates, customers, partners or other third party service providers; or (vii) use the Service in a manner that triggers a law enforcement, government, or regulatory agency to request the suspension of the Service to Customer and/or its related phone numbers.

- **Infringing Content**. Content that infringes or misappropriates the intellectual property or proprietary rights of others.

- **Offensive Content**. Content that: (i) is defamatory, illegal, obscene, offensive, inappropriate, pornographic, abusive, invasive of privacy, or otherwise objectionable, including content that constitutes child pornography, relates to bestiality, or depicts non-consensual sex acts; or (ii) is, facilitates, or encourages libelous, defamatory, discriminatory, or otherwise malicious or harmful speech or acts to any person or entity, including but not limited to hate speech, and any other material that Entrust reasonably believes degrades, intimidates, incites violence against, or encourages prejudicial action against anyone based on age, gender, race, ethnicity, national origin, religion, sexual orientation, disability, geographic location or other protected category;

- **Harmful Content**. Content or other computer technology that may damage, interfere with, surreptitiously intercept, or expropriate any system, program, or data, including viruses, Trojan horses, spyware, worms, time bombs, cancelbots, or any other malicious, harmful, or deleterious programs.

No Security Violations

You may not use the Service to violate the security or integrity of any network, computer or communications system, software application, or network or computing device, including, without limitation, the computers used to provide the Service (each, a "**System**"). Prohibited activities include:

- **Unauthorized Access**. Accessing or using any System without permission, including attempting to probe, scan, or test the vulnerability of a System or to breach any security or authentication measures used by a System.

- **Interception**. Monitoring of data or traffic on a System without permission.

- **Falsification of Origin**. Forging TCP-IP packet headers, e-mail headers, or any part of a message describing its origin or route (including creating a false phone number), or otherwise attempting to mislead others as to the origin of a message or phone call. The legitimate use of aliases and anonymous remailers is not prohibited by this provision.

- **Creating False Identity**. Creating a false identity or phone number, or otherwise attempting to mislead others as to the identity of the sender.

No Network Abuse

You may not make network connections to any users, hosts, or networks unless You have permission to communicate with them. Prohibited activities include:

- **Monitoring or Crawling**. Monitoring or crawling of a System that impairs or disrupts the System being monitored or crawled.

- **Denial of Service (DoS)**. Inundating a target with communications requests so the target either cannot respond to legitimate traffic or responds so slowly that it becomes ineffective. Launching or facilitating, whether intentionally or unintentionally, a denial of service attack on the Service or any other conduct that materially and adversely impacts the availability, reliability, or stability of the Service.

- **Computer Viruses**. Do not intentionally distribute a computer virus or in any other way attempt to interfere with the functioning of any computer, communications system, or website, including the computer, and communications systems used to provide the Service. Do not attempt to access or otherwise interfere with the accounts of customers and/or users of the Service or the Service itself;

- **Intentional Interference**. Interfering with the proper functioning of any System, including any deliberate attempt to overload a system by mail bombing, news bombing, broadcast attacks, or flooding techniques.

- **Operation of Certain Network Services**. Operating network services like open proxies, open mail relays, or open recursive domain name servers.

- **Avoiding System Restrictions or Security Mechanisms**. Using manual or electronic means to avoid, bypass or break any use limitations placed on a System, such as access and storage restrictions, or otherwise attempting to penetrate or disable any security system or mechanisms. Using the Service in any other manner that poses a material security or service risk to Entrust or any of its other customers. Reverse-engineering the Service in order to find limitations, vulnerabilities, or evade filtering capabilities.

No E-Mail or Other Message Abuse

You will not distribute, publish, send, or facilitate the sending of unsolicited mass e-mail or other messages, promotions, advertising, or solicitations (like "spam"), including commercial advertising and informational announcements. You will not alter or obscure mail headers or assume a sender's identity without the sender's explicit permission. You will not collect replies to messages sent from another internet service provider if those messages violate this AUP or the acceptable use policy of that provider.

Engaging in any unsolicited advertising, marketing or other activities prohibited by applicable law or regulation covering anti-spam, data protection, or privacy legislation in any applicable jurisdiction, including, but not limited to anti-spam laws and regulations such as the CAN SPAM Act of 2003, the Telephone Consumer Protection Act, and the Do-Not-Call Implementation Act.

Using the Service in connection with unsolicited, unwanted, or harassing communications (commercial or otherwise), including, but not limited to, phone calls, SMS or MMS messages, chat, voice mail, video, or faxes.

Messaging

What Is Proper Consent? Consent can't be bought, sold, or exchanged. For example, You can't obtain the consent of message recipients by purchasing a phone list from another party.

Aside from two exceptions noted later in this section, You need to meet each of the consent requirements listed below. You need to require that Your customers adhere to these same requirements when dealing with their users and customers.

Consent Requirements

- Prior to sending the first message, You must obtain agreement from the message recipient to communicate with them - this is referred to as "consent", You must make clear to the individual they are agreeing to receive messages of the type you're going to send. You need to keep a record of the consent, such as a copy of the document or form that the message recipient signed, or a timestamp of when the customer completed a sign-up flow.

- If You do not send an initial message to that individual within 30 days of receiving consent, then You will need to reconfirm consent (see “Double Opt-in” below).

- The consent applies only to You, and to the specific use or campaign that the recipient has consented to. You can't treat it as blanket consent allowing You to send messages from other brands or companies You may have, or additional messages about other uses or campaigns.

Alternative Consent Requirements: The Two Exceptions

While consent is always required and the consent requirements noted above are generally the safest path, there are two scenarios where consent can be received differently.

- *Contact initiated by an individual*

If an individual sends a message to You, You are free to respond in an exchange with that individual. For example, if an individual texts Your phone number asking for Your hours of operation, You can respond directly to that individual, relaying Your open hours. In such a case, the individual’s inbound message to You constitutes both consent and proof of consent.

Remember that the consent is limited only to that particular conversation. Unless You obtain additional consent, don't send messages that are outside that conversation.

- *Contact initiated by You to send informational content to an individual based on having a prior relationship*

You may send an outbound message that provides information requested by the individual, or that can be reasonably expected by the individual based on Your relationship. An example of such a relationship and message is a dentist reminding a patient of an appointment.

In addition to appointment reminders, other examples include receipts, one-time passwords, order/shipping/reservation confirmations, drivers coordinating pick up locations with riders, and repair persons confirming service call times.

The message can't attempt to promote a product, convince someone to buy something, or advocate for a social cause.

The individual must have knowingly provided their phone number to You, and have taken some action to trigger the potential for communication. Actions can include a button press, setting up an alert, making an appointment, or placing an order.

NOTE: The alternative consent requirements cannot be used for promotional content such as marketing, coupons, advertisements, notifications regarding a job opportunity, and sweepstakes, independent of whether the individual initiates contact, or You have consent for informational content of the type noted above based on a prior relationship.

Double Opt-in Consent

We require double opt-in consent in some limited use cases. Many of these use cases listed below generate the majority of complaints about unwanted messages which is why the burden of consent is higher.

- Affiliate marketing including multi-level marketing - this is typically a marketing arrangement which an online retailer pays commission to an external website for traffic or sales generated from its referrals.
- Lead generation services
- Sweepstakes
- Financial products, unless You are the financial institution directly offering the product. These include debt refinancing, short-term credit offers, and payday loans
- Job alerts
- Work-from-home offers

Double opt-in is a two-step process:

- First, the message recipient must knowingly provide consent to You or Your customer prior to receiving any text message. That consent must be provided through an electronic signature or some other online sign-up form that makes clear to the individual they are agreeing to receive messages of this type.
- Second, in Your first text message to that individual, You must identify yourself and prompt the individual to confirm their consent.

For example, Your first outbound message would be compliant if it included text similar to, “This is Company X. You recently signed up to receive text messages from us. Please reply YES to confirm or STOP to unsubscribe.” Only after You receive the confirmation “YES” may You send a follow-up message with information related to a topic listed above.

Identifying Yourself as the Sender

Every message You send must clearly identify You as the sender, except in follow-up messages of an ongoing conversation.

Message Recipient Opt-out

The initial message that You send to an individual needs to include the following language: “Reply STOP to unsubscribe,” or the equivalent using another standard opt-out keyword, such as STOPALL, UNSUBSCRIBE, CANCEL, END, and QUIT.

Individuals must also have the ability to revoke consent at any time by replying with a standard opt-out keyword. When an individual opts out, You may deliver one final message to confirm that the opt-out has been processed, but any subsequent messages are not allowed. An individual must once again provide consent before You can send any additional messages.

Periodic Messages and Ongoing Consent

In some cases, You may want to periodically send messages to an individual who earlier provided proper consent. This practice is allowed, provided that Your message includes a reminder to the individual about how to unsubscribe. If You send more than one message in a given month, You need to include the reminder in just one of those messages--not in all of the messages that You send in that month.

You must respect the message recipient's preferences in terms of frequency of contact. You also need to proactively ask individuals to reconfirm their consent no less often than once every 18 months.

Age and Geographic Gating

If You are sending messages in any way related to alcohol, firearms, gambling, tobacco, or other adult content, then more restrictions apply. In addition to obtaining consent from every message recipient, You must ensure that no message recipient is younger than the legal age of consent based on where the recipient is located. You also must ensure that the message content complies with all applicable laws of the jurisdiction in which the message recipient is located. Additionally, this AUP bans sending any content that is offensive, inappropriate, pornographic, obscene, illegal, or otherwise objectionable, even if the content is permissible by law and appropriate age restrictions are in place.

You need to be able to provide proof that You have in place measures to ensure compliance with these restrictions.

Content We Do Not Allow

The key to ensuring that messaging remains a great channel for communication and innovation is preventing abusive use of messaging platforms. That means we never allow some types of content on our platform, even if our customers get consent from recipients for that content. Those content types include:

- Anything that's illegal in the jurisdiction where the message recipient lives. For example, we do not allow messages related to the sale of recreational or medicinal cannabis in the United States, because United States federal laws prohibit its sale.

- Hate speech or harassment, or any communications from groups whose primary purpose is deemed to be spreading hate.

- Fraudulent messages.

- Malicious content, such as malware or viruses.

- Any content that is designed to intentionally evade filters.

How We Handle Violations

When we identify a violation of these principles, we work with You in good faith to get You back into compliance. To protect the continued ability of all our customers to freely use messaging for legitimate purposes, we reserve the right to remove access to the Service (or portions thereof) in accordance with the contract Disputes Clause (Contract Disputes Act) for customers that we determine are not complying with this AUP, or who are not following the law in any applicable area.

Our Monitoring and Enforcement

We reserve the right, but do not assume the obligation, to investigate any violation of this AUP or misuse of the Service. We may:

- investigate violations of this AUP or misuse of the Service; or

- remove, disable access to, or modify any content or resource that violates this AUP or any other agreement we have with You for use of the Service.

We may report any activity that we suspect violates any law or regulation to appropriate law enforcement officials, regulators, or other appropriate third parties. Our reporting may include disclosing appropriate customer information. We also may cooperate with appropriate law enforcement agencies, regulators, or other appropriate third parties to help with the investigation and prosecution of illegal conduct by providing network and systems information related to alleged violations of this AUP.

Reporting of Violations of this AUP

If You become aware of any violation of this AUP, You will immediately notify us and provide us with assistance, as requested, to stop or remedy the violation. To report any violation of this AUP, please follow our abuse reporting process.

IDENTITY AS A SERVICE

SERVICE LEVEL AGREEMENT

Unless otherwise provided herein, capitalized terms will have the meaning specified in the Entrust Identity as a Service Schedule (“**Agreement**”). Entrust reserves the right to change the terms of this Identity as a Service Service Level Agreement (“**SLA**”) in accordance with the Agreement.

1. Service Commitment

Entrust will use commercially reasonable efforts to make the Hosted Service available with a Monthly Uptime Percentage (as defined below) of at least 99.9% during each calendar month (the “**Service Commitment**”). In the event that the Hosted Service does not meet the Service Commitment, Customer may be eligible to receive a Service Credit as described below.

2. Definitions

- “**Monthly Uptime Percentage**” is calculated by subtracting from 100% the percentage of minutes during the month in which the Hosted Service was in the state of Downtime.
- “**Downtime**” means a state during which authorized Users are unable to use the Hosted Service to authenticate their identity in order to gain access to protected assets and applications.
- “**Maintenance Window**” means a time frame during which Entrust performs scheduled routine system maintenance on the Hosted Service.
- “**Service Level Default**” means an instance when Entrust’s level of performance has failed to meet the Service Commitment.
- “**Service Credit**” means a set of no cost days that can be applied against Customer’s subscription renewal costs.

3. Service Commitments and Service Credits

Service Credits are calculated as set out below for each month in which a Service Level Default occurs.

Monthly Uptime Percentage	Service Credit
Less than 99.9% but greater than 99%	3 days
Less than 99% but equal to or greater than 95.0%	5 days
Less than 95.0%	15 days

In no event will Customer’s Service Credits for any calendar year exceed 15 days.

4. Credit Request and Payment Procedures

In order to receive a Service Credit, a credit request must be received by Entrust via email to the following email address AR.Management@entrust.com within thirty (30) days of the Service Level Default and must include:

1. The words “SLA Credit Request” in the subject line;
2. The dates and times of the Service Level Default; and
3. Customer logs and test reporting showing the Service Level Default;

If requested by Entrust, Customer will work with Entrust to verify the accuracy of the logs and test reports provided to Entrust so that Entrust, acting reasonably, may confirm that the Service Level Default occurred. Customer's failure to provide the credit request and/or the information required above will disqualify Customer from receiving a Service Credit.

5. Maintenance Windows

Maintenance Windows will not exceed one (1) hour per month. Entrust will use commercially reasonable efforts to provide Customer with advance notice of any Maintenance Window.

6. Downtime Exclusions

Downtime does not include any unavailability that results from: (i) Entrust's suspension or termination of the Hosted Service; (ii) factors outside of Entrust's reasonable control, including without limitation, any force majeure event, Internet accessibility problem beyond Entrust's ISP environment, Customer's network, software, equipment or other technology; (iii) the Licensed Software hosted by Customer; and (iv) any Maintenance Window.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms")**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. "**Business Day**" means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. "**Covered Offering**" means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. "**Customer-Hosted Offering**" means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer's premises.

1.4. "**Extended Support**" means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. "**Hosted Service**" for the purposes of this Schedule means Entrust's Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. "**Incident**" means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. "**Named Support Contacts**" means individual Users nominated by Customer to act as Customer's support representatives.

1.8. "**Problem**" means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. "**Production Environment**" means Customer's live business environment with active users.

1.10. "**Response Time**" means the amount of time that elapses between the Customer's report of a Service Request to Entrust and Entrust's acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. "**Service Plan**" means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**" means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. "**Software**" for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. "**Superseded Product**" means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees.**

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer's Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail ("Immediate Incident Response Time").

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. **Upgrades for Customer-Hosted Offerings**.

8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions**.

9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services**. If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination**. In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other

party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act).

Identity Enterprise

End User License Terms and Conditions

The Agreement for Entrust's Identity Enterprise Offering ("Identity Enterprise") is comprised of these end user license terms and conditions (the "IDE Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for Identity Enterprise. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity.

IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE OFFERING. THE CONTINUED RIGHT TO ACCESS AND USE THE OFFERING IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Definitions.**

1.1. "CAL" or "Client Access License" means a license enabling or permitting the use of certain capabilities in respect to a specific individual end user or a specific Device, on a single (1) instance of the Software.

1.2. "Customer Data" means any content, data, or information (including, third-party content, data, or information) that is supplied to Entrust (or its licensors or service providers) in connection with Customer's use of the Entrust Technology. Customer Data may include Personal Data.

1.3. "Data Subject" has the meaning set out in the DPA.

1.4. "Device" means a computer, desktop, workstation, tablet, terminal, telephone, mobile phone, server or other electronic or computing device.

1.5. "Documentation" means written materials prepared by Entrust (or its licensors or service providers) relating to the Entrust Technology, including, without limitation, guides, manuals, instructions, policies, reference materials, release notes, online help or tutorial files, support communications (including any disputes between the parties) or any other materials provided in connection with modifications, corrections, or enhancements to the Entrust Technology, all as may be modified from time to time.

1.6. "Entrust Technology" means the Software and any related Documentation.

1.7. "Hardware" shall have the meaning set out in Section 2.9.1 (*Hardware (Default Provisions)*).

1.8. "Licensing String" means a data key provided by Entrust for the purpose of setting the number of CALs or otherwise enabling or controlling certain capabilities within the Software.

1.9. "Special Terms and Conditions" mean any terms and conditions attached to this IDE Schedule.

2. **Software Licenses.**

2.1. Grant of License**.** Subject to Customer's compliance with the Agreement, Entrust hereby grants Customer a personal, non-exclusive, non-transferable, non-sub-licensable license to download, install, and use the Software, in object code form only, for the sole purpose of conducting Customer's internal business operations, and not for resale or any other commercial purpose, all in accordance with: (i) the Documentation; and (ii) any specifications or limitations set out in the Order or imposed by technological means of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription or transaction levels, as well as on copies of Software, numbers or types of users or devices, number of CALs, and types of deployment (e.g. high availability, test or disaster recovery).

2.2. Licensed Not Sold. The Software is protected by copyright and other intellectual property laws and treaties. Copies of the Software provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software itself.

2.3. Upgrades. This Software Schedule does not grant any entitlement to receive any upgrades to the Software. If Customer is entitled to receive upgrades to any Software, for example as a result of purchasing maintenance and support under a separate Support Schedule or subscribing to an Offering that includes Support with upgrades for the connected Software, then such Software includes such upgrades, subject to any additional terms that may be imposed on enhanced features made available as part of the upgrade.

2.4. Restrictions. In addition to the restrictions set out in the General Terms, Customer shall not: (i) use the Software for service bureau or time-sharing purposes; (ii) permit any unauthorized third parties from accessing the Entrust Technology; or (iii) attempt to gain unauthorized access to, or disrupt the integrity or performance of, the Software or the data contained therein.

2.5. License Strings. If an item of Software uses a Licensing String, Customer shall only use such Licensing String in conjunction with the copy of Software for which it was delivered, and Customer may not copy or alter a Licensing String or use it for more than one (1) instance of the Software. All quantities are total quantities. For example, if Customer acquires a license for five (5) copies of an item of Software and acquires 10,000 CALs for such Software, then a total of 10,000 CALs can be used with the Software (i.e. Customer have not purchased 50,000 CALs).

2.6. Installation and Management. Customer agrees that it will be responsible for installing, configuring, and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software resulting from Customer's improper installation, configuration, and/or management.

2.7. Documentation. Customer may reproduce and use the Documentation solely as necessary to support Customer's access to and use of the Software. Each permitted copy of all or part of the Documentation must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust or downloaded or otherwise accessed by Customer.

2.8. Support. If an Order calls for support, any such support will be provided pursuant to the terms and conditions set out in the Support Schedule attached hereto. Notwithstanding the foregoing, where support is purchased through an authorized reseller and the Order indicates that the authorized reseller will provide support, then such support will be provided by the authorized reseller (and not Entrust). If Customer is entitled to receive upgrades to any Software as a result of purchasing maintenance and support, then such Software includes such upgrades, subject to any additional terms that may be imposed on enhanced features made available as part of the upgrade.

2.9. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Entrust Technology, including, without limitation, by protecting its passwords and other log-in information. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Entrust Technology or breach of its security and will use best efforts to stop such breach or unauthorized use.

2.10. Hardware.

2.10.1. Hardware (Default Provisions). If an Order calls for hardware and no third party or Entrust separate agreements or terms and conditions accompany them, then the Agreement shall apply to such hardware ("Hardware") along with the following terms and conditions: (i) Customer will be the importer of record for the Hardware and responsible for all freight, packing, insurance and other shipping-related expenses; (ii) risk of loss and title to the Hardware will pass to Customer upon delivery of the Hardware by Entrust or one of their respective agents to the carrier; (iii) the Hardware will be free from material defects in materials and workmanship and will conform to the published specifications for such Hardware in effect as of the date of manufacture for a period of one (1) year from the date on which such Hardware are first delivered to Customer (or for such extended warranty period as may be set out in the applicable Order); and (iv) Customer will use Entrust as Customer's point of contact for Hardware warranty inquiries. The aforementioned Hardware warranty will not apply where the issue is caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Hardware. Any Hardware that is replaced becomes the property of Entrust. Entrust's exclusive liability and Customer's exclusive remedy for breach of this Section (*Hardware (Default Provisions)*) is for Entrust, at its option, to repair or replace the Hardware, or take return of the Hardware and refund the price paid for the Hardware. "Hardware" is not part of the Entrust Technology.

2.10.2. Use Only with Software. Any Hardware included with the Software may be used only with the applicable Software, unless otherwise permitted in the applicable agreement accompanying such Hardware, or as otherwise permitted by Entrust in writing.

2.11. Delivery. Entrust shall make the Entrust Technology available for electronic download within thirty (30) days of acceptance of an Order, subject to the receipt of all required documentation, including any required export and import permits. Customer will be the importer of record for the Software.

3. **Evaluation; NFR.**

3.1. Evaluation Purposes. Entrust may grant Customer the right to download, install, access, and use the Entrust Technology for evaluation purposes for the Trial Period. During the Trial Period Customer shall not (i) use the Entrust Technology in order for Customer to generate revenue; or (ii) use any Customer Data or Personal Data in its evaluation of the Entrust Technology - only fictitious non-production data can be used.

3.2. Not-for-Resale (NFR) Purposes. Entrust may grant Customer that is an authorized reseller of the Entrust Technology the right to download, install, access, and use the Entrust Technology for not-for-resale (NFR) purposes for the NFR Period. During the NFR Period Customer may download, install, access, and use the Entrust Technology for purposes of development, testing, support, integration, proofs of concept and demonstrations. Customer shall not use any Customer Data or Personal Data in its NFR use of the Entrust Technology - only fictitious non-production data can be used.

3.3. Trial Period. Customer's evaluation of the Entrust Technology pursuant to this Section 3 (*Evaluation; NFR*) shall commence on the date Customer downloads and/or accesses the Entrust Technology and continue for a period of thirty (30) days ("Trial Period"), or as otherwise agreed to by Entrust in writing with Customer (authorized reseller).

3.4. NFR Period. Customer's access to and use of the Entrust Technology for NFR purposes pursuant to this Section 3 (*Evaluation; NFR*) shall commence on the date Customer downloads and/or accesses the Entrust Technology and continue for the duration indicated in the Order or the Documentation ("NFR Period").

3.5. Termination. Notwithstanding the foregoing, Entrust may in its sole discretion terminate Customer's evaluation or NFR access to and use of the Entrust Technology at any time, for any or no reason, without advanced notice.

4. **Fees.**

4.1. Customer will pay the costs and fees (including where overages are applicable, any overage fees) for the Software (or Hardware, if applicable) as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

5. **Data Processing.**

5.1. Consents Customer Data; Personal Data. Customer represents and warrants that before providing Customer Data or Personal Data to Entrust, Customer will have provided and/or obtained the requisite consents (if any) and made all requisite disclosures (if any) to data subjects, in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data, by Entrust (or its licensors or service providers) in accordance with the Agreement. Customer shall be responsible for the accuracy, quality and legality of Customer Data or Personal Data and the means by which Customer acquired them.

6. **No Other Rights Granted; Feedback.**

6.1. No Other Rights Granted. The rights granted under the Agreement are only as expressly set forth in the Agreement. No other right or interest is or will be deemed to be granted, whether by implication, estoppel, inference or otherwise, by or as a result of the Agreement or any conduct of either party under the Agreement. Entrust and its licensors expressly retain all ownership rights, title, and interest in the products and services provided by Entrust (including any modifications, enhancements and derivative works thereof). Any permitted copy of all or part of any item provided to Customer must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust to Customer.

6.2. Feedback. "Feedback" refers to Customer's suggestions, comments, or other feedback about the Entrust Technology or other Entrust products and services. Even if designated as confidential, Feedback will not be subject to any confidentiality obligations binding Entrust. Customer hereby agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust all of Customer's right, title, and interest thereto, including without limitation intellectual property rights. Entrust acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

7. **Warranty; Disclaimer.**

7.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery the Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

7.2. Warranty Exclusions. The warranty in Section 7.1 (*Software Warranty*) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the

Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Software; (iii) any modifications or additions made to the Software by Customer. Entrust shall have no obligation to fix errors in the Software caused by accident, misuse, abuse, improper operation, misapplication, or any other cause external to the Software; or (iv) any evaluation or NFR use pursuant to Section 3 (*Evaluation; NFR*).

7.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (*Warranty*) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7.4. **Except as expressly stated in this Section 7 (Warranty), the disclaimers in Section 13 (Disclaimer of Warranties) of the General Terms apply to the Software.**

8. **Indemnification**.

8.1. Reserved.

9. **Term and Termination.**

9.1. Term**.** The Agreement will commence upon Customer's acceptance of the Agreement and, unless otherwise terminated pursuant to the Agreement, will expire on (i) the date the Trial Period or NFR Period expires; or (ii) for so long as Customer continues to use the Software in the case of a perpetual license (as applicable, the "Term").

9.2. Termination. In addition to the termination rights in the General Terms:

9.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

9.2.2. Customer may terminate a perpetual license to Software granted under this IDE Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

10. **General.**

10.1. Order of Precedence. In the event of a conflict or differences between this IDE Schedule and Special Terms and Conditions, the Special Terms and Conditions will prevail over any conflicting provisions.

10.2. Publicity. Customer agrees that Entrust may identify Customer as a customer of the Software, and, subject to its prior review and approval of a proposed copy, Entrust may issue a press release and/or case study regarding Customer's use of the Software.

10.3. U.S. Government End-Users. Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 227.7202-4 (for Department of Defense licenses only) and 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (*U.S. Government End-Users*) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (*U.S. Government End-Users*) in writing.

10.4. Audit Rights**.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement, including, without limitation, with respect to the number of (i) copies of Software made or used by Customer; and (ii) CALs issued and used ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours and subject to Government security requirements, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit. In addition to the foregoing, Entrust shall also have the right to request that Customer provide a written report setting out the number of (i) copies of Software made or used by Customer; and (ii) CALs issued and used.

10.5. Professional Services. If Entrust provides any professional services and deliverables with respect to the Entrust Technology, such professional services and deliverables shall be subject to a separate agreement between Entrust and Customer, which may set out the scope and details of any professional services and deliverables, including, if and as applicable, resource specialist(s), milestones, delivery dates, acceptance criteria, payment terms and any other information and terms related thereto.

Device Reputation

Special Terms and Conditions

These Device Reputation Special Terms and Conditions ("Device Reputation Special Terms") are attached to the Entrust Identity Enterprise Schedule ("IDE Schedule"), and contain the terms and conditions that govern access to and use of the Device Reputation Service (as defined herein). Capitalized terms not defined in Section 1 herein or elsewhere in these Device Reputation Special Terms shall have the meaning set out in the IDE Schedule. References to articles or sections herein shall be to articles or sections in these Device Reputation Special Terms unless otherwise expressly stated. Provisions in these Device Reputation Special Terms will prevail with respect to the Device Reputation Service over any conflicting provision in the IDE Schedule.

1. **DEFINITIONS.**

1.1. "Customer Application" means the application developed by Customer pursuant to the Device Fingerprint SDK License to be used to access and use the Device Reputation Service.

1.2. "Customer Data", in addition to its meaning in the IDE Schedule, with respect to the Device Reputation Service means Device Information, Risk Information, as well as data or information collected using the Customer Application.

1.3. "Database" means the centralized Global Intelligence Platform owned, operated and maintained by Entrust (or its licensors or service providers) which contains Device Information and associated information including Risk information.

1.4. "Device" means a particular computer, mobile phone, desktop, tablet or other computing device.

1.5. "Device Fingerprint" means a set of attributes and characteristics designed to identify a Device.

1.6. "Device Information" means a set of Device attributes and characteristics that are designed to identify a particular Device.

1.7. "Device Reputation Service" means the Device Reputation Service which forms part of the Entrust Technology (if selected by Customer and approved by Entrust in an Order).

1.8. "Purpose" means authentication, and assessing risk associated with end user devices (including, without limitation, transaction, abuse, reputation, and fraud risk).

1.9. "Response" means the recommendation, including Risk Information, returned by the Device Reputation Service about a Device which has been evaluated by the Device Reputation Service.

1.10. "Risk" means risk including, without limitation, transaction, abuse, reputation and fraud risk.

1.11. "Risk Information" means information relating to specific Risk(s).

1.12. "Device Fingerprint SDK License" means the Entrust Device Fingerprint SDK License through which Customer may obtain a license to use the Device Fingerprint software development toolkit. The Device Fingerprint SDK License is not a part of the Agreement.

1.13. "User" means any Data Subjects who owns or controls the Device and whose data is being collected through the Device Reputation Service.

2. USE OF DEVICE REPUTATION SERVICE.

2.1. Grant of License. Subject to Customer's compliance with the Agreement, Entrust grants to Customer, during the Device Reputation Term (as defined herein), a worldwide, non-exclusive, nontransferable, non-sub-licensable right to, all in accordance with the Documentation, the right to access and use the Device Reputation Service, for the purpose of collecting and processing Device Information and providing Responses to Customer. The foregoing right to use shall be contingent on Customer (i) paying the additional fees related to the Device Reputation Service as set out in the relevant Order; (ii) obtaining all necessary User consents to allow Entrust and its Affiliates and their respective licensors and service providers to: (a) collect and process Device Fingerprints for the Purpose; (b) make use of other internal end user identifiers for the Purpose; and (c) return the results from the processing outlined in (a) ("Results") to Customer.

2.2. Restrictions. Device Fingerprints and Results must only be used in connection with the Software and for the Purpose.

3. CUSTOMER DATA & PRIVACY.

3.1. Customer further grants to Entrust (or its Affiliates, and any of their respective licensors and service providers), a world-wide, limited right, during the Device Reputation Service Term, to host, copy, transmit and display Customer Data and Personal Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective licensors and service providers) to provide Device Reputation Service in accordance with the Agreement.

3.2. Consents; Accuracy; Rights. Customer represents and warrants that, before authorizing a User to use Device Reputation Service and before providing Customer Data or Personal Data to Entrust, Customer will have provided and/or obtained the requisite rights, consents or permissions, and made all requisite disclosures (if any), to Users in accordance with all applicable laws, rules or regulations for the collection, use, and disclosure of the Customer Data or Personal Data contained therein, by Entrust (including any of its Affiliates, and any of their respective licensors and service providers) in accordance with the Agreement. Customer further represents and warrants to Entrust that such Customer Data or Personal Data is accurate and up-to-date (and that Customer shall correct or update it as required), and that no Customer Data or Personal Data will violate or infringe (i) any third-party intellectual property, publicity, privacy or other rights; (ii) any applicable laws, rules or regulations; or (iii) any third-party products or services terms and conditions. Customer will be fully responsible for any Customer Data or Personal Data submitted, uploaded, or otherwise provided to Device Reputation Service by any User as if it was submitted, uploaded, or otherwise provided by Customer. Customer is solely responsible for the accuracy, content and legality of all Customer Data and Personal Data.

3.3. Rights in Customer Data and Personal Data. As between the parties, Customer will retain all right, title and interest (including any and all intellectual property rights) in and to the Customer Data and Personal Data provided to Entrust. Subject to the terms of the Agreement, Customer hereby grants to Entrust a non-exclusive, worldwide, royalty-free right to use, copy, store, transmit, modify, create derivative works of and display the Customer Data and Personal Data contained therein solely to the extent necessary to provide Device Reputation Service to Customer, and to sub-license such rights to any of Entrust's applicable licensors and service providers.

3.4. Rights in Certain Data (Device Reputation). As between the parties, Entrust owns and will retain all right, title and interest (including but not limited to any copyright, patent, trade secret, trademark or other proprietary and/or intellectual property rights) in and to Device Reputation Service, and the Device Information, Database, and any Response. For clarity, the foregoing does not mean that Entrust owns or retains any right, title or interest in or to the data elements comprising the Device Information, the Database, or any Response. The foregoing is an acknowledgement that, as between the parties, Entrust will retain any right, title and interest it may have in the Device Information, Database, and any Response, as collective works. Customer acknowledges that the Device

Information and the Database, as collective works, may be Confidential Information of Entrust.

4. **CUSTOMER'S RESPONSIBILITIES, RESTRICTIONS & ACKNOWLEDGEMENTS**.

4.1. Compliance with Laws. Customer represents, warrants and covenants that is shall (i) use commercially reasonable efforts to prevent unauthorized access to, or use of, Device Reputation Service and shall notify Entrust as soon as possible if it becomes aware of any unauthorized access or use of Device Reputation Service; (ii) use Device Reputation Service only for lawful purposes; (iii) not knowingly violate any law of any country with its use of Device Reputation Service; and (iv) not knowingly violate the intellectual property rights of any third party with its use of Device Reputation Service.

4.2. Users; Device Reputation Service Access. . Customer is responsible and liable for: (a) handling, use, and/or consequences or impact of Results or Responses resulting from use of Device Reputation Service (e.g. impact on User's credit rating or ability to open accounts or any other unfavorable impact).

5. **TERM, TERMINATION & SUSPENSION**.

5.1. Termination or Suspension for Cause. Entrust may, at its sole discretion, temporarily suspend Customer's and/or Users' access to Device Reputation Service at any time, without advanced notice, if Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers' and/or users' information or data processed by Device Reputation Service. Entrust may also, without notice, suspend Customer's and/or User's access to Device Reputation Service for scheduled or emergency maintenance. Termination of these Device Reputation Special Terms will not necessarily result in termination of the entire Agreement (e.g. if Customer has an Identity Enterprise license and the applicable Order may still be active).

6. **INDEMNITIES**.

6.1. Reserved.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms")**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **<u>Definitions</u>.** The following terms shall have the meaning ascribed to them as follows:

1.1. "**Business Day**" means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. "**Covered Offering**" means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. "**Customer-Hosted Offering**" means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer's premises.

1.4. "**Extended Support**" means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. "**Hosted Service**" for the purposes of this Schedule means Entrust's Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. "**Incident**" means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. "**Named Support Contacts**" means individual Users nominated by Customer to act as Customer's support representatives.

1.8. "**Problem**" means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. "**Production Environment**" means Customer's live business environment with active users.

1.10. "**Response Time**" means the amount of time that elapses between the Customer's report of a Service Request to Entrust and Entrust's acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. "**Service Plan**" means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**" means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. "**Software**" for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. "**Superseded Product**" means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **<u>Support Provision</u>.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees.**

   5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

   5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

   6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

   6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

   6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

   6.4. When making a Service Request, Customer shall provide:

      6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

      6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

      6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

   6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

   6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer's Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail ("Immediate Incident Response Time").

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. **Upgrades for Customer-Hosted Offerings**.

8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide

Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions.**

9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act).

Managed PKI
Terms of Use

The Agreement for Entrust's Managed PKI Offering is made up of these terms of use (the "mPKI Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for mPKI. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE HOSTED SERVICES. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICES IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Definitions**.

1.1. "Certificate" means a digital document that, at a minimum: (a) identifies the certification authority ("CA") issuing it, (b) names or otherwise identifies a subject, (c) contains a public key of a key pair, (d) identifies its operational period, and (e) contains a serial number and (f) is digitally signed by the CA. Certificates issued by a root CA to an issuing CA are "CA Certificates".

1.2. "Customer Content" means any data, text or other content that Customer or any User transfers to Entrust for processing, storage or hosting by the Hosted Service and any computational results that Customer or any User derives from the foregoing through its use of the Hosted Service.

1.3. "Device" means an electronic endpoint in a network, system, or application, such as a computer, laptop, terminal, workstation, server, pager, telephone, smartphone, tablet, virtual workload, or other physical object enabled through embedded technology to execute functions and collect and exchange data.

1.4. "Hosted Service" means, in this mPKI Schedule, the specific mPKI and associated elements and services, that Customer has purchased as specified in the Order.

1.5. "mPKI" means a public key infrastructure consisting of software and processes hosted and managed by Entrust.

1.6. "Management Account" means a self-service administration tool hosted by Entrust that identifies Customer by its full legal name in the "Customer Name" field, tracks Customer's entitlements with respect to the Hosted Service and enables Customer, as applicable in accordance with its entitlements, to administer Hosted Service components and functions.

1.7. "PKI Policy and Practices Documentation" means, collectively, the most recent versions of the policy/ies setting out the requirements and rules applicable to a Certificate issued by an mPKI, the practices statements applicable to an mPKI or components thereof, and any guides issued by Entrust detailing the roles and responsibilities of different participants in an mPKI. The PKI Policy and Practices Documentation applicable to a specific Certificate and/or mPKI depends on the type and nature of the Certificate and of the mPKI.

1.8. "Relying Party" means a Person that relies on a Certificate and/or any digital signatures verified using that Certificate.

1.9. "Subject" means the Person or Device identified in the "Subject" field in a Certificate.

1.10. "Subscriber" means the Person who applies for or is issued a Certificate.

1.11. "User" has the meaning set out in the General Terms, and in this mPKI Schedule, includes Customer's

Affiliates and any Person who holds a role under applicable PKI Policy and Practices Documentation, an mPKI Administrator (as defined below), or a Subscriber or Subject of any Certificates issued or managed by the Hosted Service.

2. **Hosted Service Details**.

2.1. Professional Services. Entrust may provide set-up, onboarding and/or other Professional Services for some deployments of the Hosted Service, as specified in an Order, in which case the Professional Services will be provided in accordance with the applicable Order, the General Terms, and, if applicable, a Schedule describing the particular bundle of Professional Services purchased.

2.2. Hosted Service Provision. Following the completion of the set-up and onboarding of the Hosted Service, Entrust will provide and operate the Hosted Service in accordance with the Documentation, Customer's Order(s) for the Hosted Service, and in accordance with the applicable PKI Policy and Practices Documentation.

2.3. Compliance and Security Measures. Entrust will implement and maintain commercially reasonable physical and procedural security controls for the Hosted Service. Entrust will operate the Hosted Service in ISO 27001 compliant facilities according to the operational standards and procedures laid down in accordance with Entrust's corporate security policies and the applicable PKI Policy and Practices Documentation.

2.4. Service Levels. Entrust's service level commitments for the Hosted Service are as set out in the Entrust Managed PKI Services Service Levels document attached hereto.

3. **Grant of Rights**. Customer receives no rights to the Hosted Service other than those specifically granted in this Section 3 (Grant of Rights).

3.1. General. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Service, and to grant its Users the ability to access and use the Hosted Service, and to distribute Certificates issued by the Hosted Service in each case (a) in accordance with this mPKI Schedule, and, if and as applicable, the PKI Policy and Practices Documentation; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Hosted Service that Customer is permitted to use, such as limits associated with subscription levels, on numbers or types of Certificates, identities, Users, signatures or Devices, and on types of deployment (e.g. high availability, test or disaster recovery); and (d) subject to the restrictions set out in Section 3 of the General Terms (Restrictions).

3.2. Evaluation. At Entrust's discretion, it may provide Customer with access to and right to use the Hosted Service for evaluation purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Section 3.2 (Evaluation) or a separate evaluation agreement executed by the parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms, this mPKI Schedule, and an applicable Order (if any), for the period specified by Entrust at its discretion Customer may, solely as necessary for Customer's evaluation of the Hosted Service, access and use the Hosted Service exclusively in and from a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data). Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.1 (Professional Services), 2.2 (Hosted Service Provision), 3.1 (General), 6 (Support), 11.1 (Term) and 13 (Publicity) do not apply to any evaluation of the Hosted Service. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Service at any time, for any or no reason, without advance notice.

4. **Customer Roles and Responsibilities**.

4.1. mPKI Participants and Roles. Customer will have one or more roles in the Hosted Service, and will fulfill the responsibilities and functions of such roles as set out in the applicable PKI Policy and Practices Documentation. In addition, Customer will appoint trusted Users into additional roles ("mPKI Administrators"), and will be responsible for ensuring that such mPKI Administrators fulfill the responsibilities and functions of their roles as set out in the applicable PKI Policy and Practices Documentation, including in the verification of Certificate applications and the administration of Subscribers. Customer agrees that Entrust is entitled to rely on instructions provided by the mPKI Administrators with respect to the Hosted Service as if such instructions were provided by the Customer itself.

4.2. Users and Other Third Parties. Customer will make no representations or warranties regarding the Hosted Service or any other matter, to Users, Relying Parties and/or any other third party, for or on behalf of Entrust, and Customer will not create or purport to create any obligations or liabilities on or for Entrust regarding the Hosted Service or any other matter. Entrust may direct any requests or other communications by Relying Parties or Users to Customer.

4.3. On-premise Components. If Customer's Order for the Hosted Service includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Service (collectively, "Customer-hosted Products") Customer will be responsible for the lifecycle management (patching, upgrades, etc.) of such Customer-hosted Products and the security of the environment where it installs and uses such Customer-hosted Products. Customer will implement at a minimum such security measures with respect to the Customer-hosted Products and the environment where it is installed as set out in the applicable PKI Policy and Practices Documentation. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures, including maintaining the communication workstation(s) in a physically-secure room with access restricted to a limited number of named persons; (ii) ensure that persons employed by or contracted to work with the Customer-hosted Products on behalf of Customer have appropriate skills, knowledge, and backgrounds (including any security clearance requirements imposed by law or Government policy) to operate in a trusted and secure environment; and (iii)for any Customer-hosted Products that are or include software, always use the current version of such software and promptly install any security patches and any upgrades/updates required for proper functioning of all features of the Hosted Service. Customer understands if it fails to comply with this Section it would create a security risk and/or otherwise negatively impact the operation of the Hosted Service and Entrust will have the right to suspend the Hosted Service in accordance with Section 13 (Suspension). In addition, Customer may not be able to access new features or functions of the Hosted Service if it does not comply with this Section.

4.4. Network Requirements. Customer is responsible for procuring, maintaining, monitoring and supporting its communications infrastructure, network (LAN or WAN), and all components that connect to the Hosted Service(s), including facilities to terminate VPN tunnels as specified by Entrust. Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure, nor for any service degradation or failures caused by network connectivity of such external infrastructure.

4.5. Devices. For Certificates issued to Devices, Customer is responsible for ensuring that the relevant Devices support and are interoperable with the Certificates.

4.6. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Hosted Service, including, without limitation, by securing, protecting and maintaining the confidentiality of its access credentials and any access credentials issued to its Users. Customer is responsible for any access and use of the Hosted Service via Customer's Management Account and for all activity that occurs in Customer's Management Account. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Service or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

4.7. Data Safeguards. Customer is responsible for determining whether the Hosted Service offers appropriate safeguards for Customer's intended use of the Hosted Service, including any safeguards required by applicable laws, prior to transmitting or processing, or prior to permitting Users to transmit or process, any data or communications via the Hosted Service.

5. **Software.** If Entrust provides any Software in connection with the Hosted Service, the Schedule provided with the Software will apply (and not this mPKI Schedule, with the exception of Section 4.3 (On-premise Components)). If no more specific Schedule is provided with the Software, the Schedule for the Software attached to this Schedule.

6. **Open Source**. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

7. **Support.** Entrust provides the support commitments set out in the Support Schedule attached to this Schedule for the Hosted Service and any Software provided in connection with the Hosted Service. The "Silver Support Plan", as described in the Support Schedule, is included at no additional charge with a subscription to a Hosted Service. Other levels of Support may be available for purchase for an additional fee.

8. **Interoperability.** Entrust or third parties may make available plugins, agents, or other tools that enable the Hosted Service to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Hosted Service, are licensed separately, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Service with such Interoperation Tools under this mPKI Schedule. If Customer uses any Interoperation Tool, Customer has exclusive responsibility to ensure that it has any and all requisite rights to use the Interoperation Tool, including using it to transfer any data from or to the Hosted Service, and to use the product or service with which it connects. The use of an Interoperation Tool does not create any data subprocessor relationship between Entrust and any third party.

9. **Hardware.** If the Order specifies any Hardware and Supplies to be delivered to Customer by Entrust or one of its suppliers in connection with the Hosted Service, the Hardware and Supplies Schedule attached hereto will apply, unless the Hardware and Supplies are Third Party Vendor Products, in which case Section 15.1 of the General Terms (Third Party Vendor Products) will apply.

10. **Reserved**..

11. **Fees.** Customer will pay the costs and fees for the Hosted Service as set out in the applicable Order in accordance with the GSA Schedule Pricelist, which are payable in accordance with the Order and the General Terms.

12. **Term & Termination**.

    12.1. Term. The Hosted Service is sold on a subscription basis for the Offering Term set out in the applicable Order.

    12.2. Termination. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

    12.3. Effects of Termination. Without limiting the generality of the effects of termination set out in the General Terms, upon termination of the Hosted Service, the CAs forming part of the Hosted Service will be inaccessible, Entrust will cease providing status reporting and may revoke the CA Certificates, and Customer's rights to use or access the Hosted Service, including the ability to use the Hosted Service to revoke Certificates, will cease. Customer understands that any use or reliance on unrevoked Certificates is entirely at Customer's own risk.

13. **Suspension**. In the event that Entrust suspects any breach of the Agreement or the PKI Policy and Practices Documentation by Customer and/or Users, Entrust may temporarily suspend Customer's, and/or such Users'

access to and use of the Hosted Service without advanced notice, in addition to such other remedies as Entrust may have pursuant to the Agreement. Nothing in the Agreement requires that Entrust take any action against any Customer, User or other third party for violating the Agreement, but Entrust is free to take any such action at its sole discretion.

14. **Publicity**. Customer agrees to participate in Entrust's press announcements, case studies, trade shows, or other marketing reasonably requested by Entrust. During the Term and for thirty (30) days thereafter, Customer grants Entrust the right, free of charge, to use Customer's name and/or logo, worldwide, to identify Customer as such on Entrust's website or other marketing or advertising materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope.**

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the

Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery.** Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty.**

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination.**

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users.** Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source.** Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Entrust Managed PKI Services
Service Levels

These service levels provisions are incorporated into any Agreement between Entrust and Customer consisting of (i) the Entrust General Terms and Conditions ("General Terms"); (ii) an Order for any of the Entrust Offerings identified in Section 1 of this document below (each, an "Offering"); and (iii) the applicable Offering Schedule. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Offering Schedule. Entrust may revise these service levels and support provisions by posting a new version at https://www.entrust.com/legal-compliance/terms-conditions. Such new version will become effective on the date it is posted except that if the new version significantly reduces Customer's rights, it will become effective sixty (60) days after being posted. If Customer objects in writing during that sixty (60) day period, the new version will become effective upon renewal of Customer's subscription.

1. **Service Level Targets.** Entrust will use commercially reasonable efforts to achieve the targets set out below (each, a "Service Level Target"):

Offering	Applicable Components/Functions	Target
Entrust Managed PKI PRO and PRO+ (dedicated CA infrastructure)	Certificate issuance and revocation (CA and RA services hosted by Entrust)	99.5% Uptime
Managed Microsoft PKI	Microsoft Active Directory Certificate Services (MS PKI) – Running in Azure PKI: • Microsoft Certificate Authority • Microsoft Network Device Enrollment Service (NDES) • Certificate Services Web Enrollment • Certificate Revocation List Distribution Point (CRL DP) • Active Directory (AD) • Hardware Security Modules (HSMs)	99.5% Uptime
Certificate validation services	OCSP and CRLs	99.9% Uptime
Cryptography-as-a-Service	HSM cluster availability (excludes site-to-site VPN connectivity)	99.9% Uptime
Managed Certificate Hub	user console with dashboard, reports, notifications, Certificate visibility, configuration management connecting to CAs, sources and destination plugins (excludes site-to-site VPN connectivity)	99.5% Uptime
All	Test components (including test CAs) All components of Offerings provided for evaluation purposes	n/a

2. **Calculation of Uptime.**

2.1. "Uptime" is calculated for each calendar month by subtracting the percentage of Downtime during such month from 100%.

2.2. "Downtime" means, subject to the exclusions below, an interruption of five (5) minutes or more during which the ability of ten percent (10%) or more of all users of the applicable Offering(s) to access one or more of the components or functions listed in Section 1 above is substantially impaired.

3. **Maintenance Windows and Other Exclusions from Downtime.**

3.1. “Maintenance Windows” are the time frames during which Entrust may perform scheduled routine system maintenance. The Maintenance Windows will not exceed 12 hours per month. Entrust will use commercially reasonable efforts to provide 7 days advance notice of the Maintenance Windows.

3.2. Unavailability due to any of the following is excluded from Downtime: (i) any Maintenance Windows, (ii) suspension or termination of the applicable Offering in accordance with the terms of the applicable Agreement; (ii) implementation of critical / emergency security patches in accordance with a relevant risk/vulnerability assessment; (iii) factors outside of Entrust’s reasonable control, including any Force Majeure event, internet accessibility problems beyond Entrust’s ISP environment; and (iv) Customer’s or any third party’s network, software, equipment or other technology or service.

4. **Notice of Default.**

4.1. In order to receive a Service Level Credit (as defined below), Customer must provide written notice to Entrust within thirty (30) days of the end of the month in which the failure occurred if Customer believes Entrust has failed to meet any Service Level Target (“Service Level Default”). Upon receipt of such notice, Entrust will verify the accuracy of details provided by Customer against its service logs to determine, acting reasonably, whether a Service Level Default has or has not occurred, and will provide details relating to the cause of the Service Level Default to Customer within thirty (30) days from the date of notification. Customer’s failure to provide the notice required in this Section will disqualify Customer from receiving a Service Level Credit.

5. **Service Level Credit.**

5.1. Customer will be entitled to receive the Service Level Credit for a confirmed Service Level Default.

5.2. “Service Level Credit” means an amount equal to five percent (5%) of the Monthly Fee for the calendar month in which a Service Level Default occurs, where “Monthly Fee” means the subscription fees paid to Entrust for the Offering divided by the number of months in the applicable subscription term.

5.3. The total aggregate amount of the Service Level Credit to be issued by Entrust to Customer for all Service Level Defaults that occur in a single calendar month will be capped at five percent (5%) of the Monthly Fee for such calendar month. Service Level Credits can only be applied against the renewal subscription fees due to Entrust for the Offering and any unused Service Level Credits arhardwe forfeited upon termination or non-renewal of the Agreement. For clarity, Entrust is not required to issue refunds or make payments against such Service Level Credits under any circumstances, including upon termination of the Agreement. The Service Level Credit is Customer’s sole and exclusive remedy for any Service Level Default.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the "Support Schedule"), the Entrust General Terms and Conditions ("General Terms")**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. "**Business Day**" means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.

1.2. "**Covered Offering**" means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.

1.3. "**Customer-Hosted Offering**" means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer's premises.

1.4. "**Extended Support**" means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.

1.5. "**Hosted Service**" for the purposes of this Schedule means Entrust's Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.

1.6. "**Incident**" means a Service Request that has been classified as Severity 1 in accordance with this Schedule.

1.7. "**Named Support Contacts**" means individual Users nominated by Customer to act as Customer's support representatives.

1.8. "**Problem**" means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.9. "**Production Environment**" means Customer's live business environment with active users.

1.10. "**Response Time**" means the amount of time that elapses between the Customer's report of a Service Request to Entrust and Entrust's acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

1.11. "**Service Plan**" means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

1.12. "**Service Request**" means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.13. "**Software**" for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.14. "**Superseded Product**" means previous version(s) of the Software or Third Party Vendor Product(s).

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

1.16. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees.**

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer’s Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. “Second Line Support” means (i) communicating with Customer’s Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust’s control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail (“Immediate Incident Response Time”).

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust’s sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust’s Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer’s business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan.

The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. **Upgrades for Customer-Hosted Offerings**.

8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions**.

9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services**. If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination**. In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act).

Hardware and Supplies Schedule

If Entrust provides any Hardware and Supplies in connection with an Order, then the following terms apply with respect to the Hardware and Supplies portion of the Offering. Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Shipment; Title and Risk of Loss.** Unless otherwise specified in this Agreement: (i) Hardware and Supplies will be shipped at Entrust's sole discretion either EXW Entrust's dock or FCA Entrust's dock ("INCOTERMS 2020"): (ii) Customer is responsible for obtaining all insurance needed and for all shipping charges; (iii) Hardware and Supplies are deemed to be accepted by the Customer upon delivery in accordance with the INCOTERMS 2020 stated above; and (v) Customer is responsible for installation of the Hardware and Supplies. Legal title and risk of loss of or damage to the Hardware and Supplies pass from Entrust to Customer upon delivery to the shipping carrier in accordance with the applicable INCOTERMS 2020.

2. **Warranties.** Entrust makes no warranties with respect to the Hardware and Supplies or Software associated to Hardware and Supplies other than as set forth in this Schedule or as may be set forth in the documentation delivered by Entrust with the Hardware and Supplies ("Warranty Documentation"), which warranties are subject to the limitations set forth in this paragraph. Entrust warrants that i) Software associated to Hardware and Supplies will perform in accordance with specification set out in the related Documentation for a period of ninety (90) days from the date of delivery; and ii) Hardware and Supplies will be free from defects in material and workmanship for one year unless otherwise set forth in the Warranty Documentation. The remedy for breach of the aforesaid warranty is limited to the repair or replacement of the defective item at no charge to Customer or the refund of the purchase price of the item, at Entrust's sole option, and is conditioned upon (i) Customer's payment of the price or fee specified in an applicable Order (except for purchases via authorized resellers); (ii) the proper use, maintenance, management and supervision of the item; (iii) the exclusive use of Hardware and Supplies or consumable materials supplied by Entrust for the item; (iv) a suitable operating environment for the item; and (v) the absence of any intentional or negligent act or other cause external to the item affecting its operability or performance. This warranty will be null and void if maintenance is performed on a Hardware and Supplies by any party other than Entrust or a qualified party approved by Entrust or if any addition to, removal from or modification of the Hardware and Supplies is made without Entrust's approval. Once they have been replaced, all parts removed from Hardware and Supplies under warranty will become the property of Entrust. If Entrust is requested to provide maintenance service for the Hardware and Supplies that is not covered by the stated warranty, Customer will be responsible for the cost of all such service at Entrust's then-current time and materials rates.

3. **Waste Electrical and Electronic Equipment.** For sales made in the European Union, the Customer alone shall be responsible for, and shall bear the cost of the collection, treatment, recovery and environmentally sound disposal of waste electrical and electronic equipment for the purposes of any decree, statute, regulations, order or other legislation which implements the terms of Directive 2012/19/EU on Waste Electrical and Electronic Equipment in the member state concerned.

4. **Software (and Firmware) License Associated to Hardware and Supplies.** Customer's rights related to Software (and Firmware) Associated to Hardware and Supplies are established by and limited to the terms and conditions specified in the End User License Agreement (EULA) accompanying the Hardware and attached to this Schedule.

5. **Support**. Entrust provides the service levels and Support Services for the Hardware and Supplies (including Software Associated to Hardware and Supplies) as set out in the Support Schedule or a separate Support agreement, a copy of which is available at request. Where Support is purchased through an authorized reseller and the Order indicates that the reseller will provide Support, such support will be provided by the authorized reseller.

6. **Issuance HSM**. If Customer has purchased an Issuance HSM, Customer is strictly prohibited from using the Issuance HSM as a general purpose HSM and may only use the Issuance HSM for the limited purposes of supporting Entrust's 'Issuance' products. An "Issuance HSM" means a hardware security module ("HSM") that that has been purchased and/or licensed specifically for supporting Entrust's credit card Issuance products.

nShield as a Service Direct Schedule

The Agreement for Entrust's nShield as a Service Direct Offering ("nSaaS Direct") is made up of these terms and conditions (the "nSaaS Direct Schedule"), the Entrust General Terms and Conditions ("General Terms") and an Order for nSaaS Direct. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity.

IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE NSAAS DIRECT. THE CONTINUED RIGHT TO ACCESS AND USE NSAAS DIRECT IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **Definitions.** The following capitalized terms have the meanings set forth below whenever used in this nSaaS Direct Schedule.

1.1. "Customer Data" means any data, information, or other content that Customer transfers to Entrust for processing, storage or hosting by the Hosted Service. Customer Data excludes Service Data.

1.2. "Customer Enrollment Form" means the Entrust online or written nSaaS Direct enrollment form signed and completed by Customer and confirmed by Entrust.

1.3. "Documentation" means written materials prepared by Entrust (or its licensors or service providers) relating to the Hosted Service, including, without limitation, guides, manuals, instructions, policies, reference materials, release notes, online help or tutorial files, support communications (including any disputes between the parties) or any other materials provided in connection with modifications, corrections, or enhancements to the Hosted Service, all as may be modified from time to time.

1.4. "Enrollment Services" means the initial set of activities carried out by Entrust to enroll Customer and enable deployment of the Hosted Service, as further described in Section 2.7 (*Enrollment Services*).

1.5. "Fully Managed" or "Security World Management" means an service that a Customer may subscribe to, where Entrust, on behalf of Customer, (i) hosts the Hosted Service; (ii) is responsible for the administration of the Security World; (iii) acts as the Security Officer performing administrative duties requiring Security Officer authorization; and (iv) is responsible for the configuration of the HSMs relevant to the Hosted Service. Entrust shall also retain Security World artefacts such as smartcards or configuration files.

1.6. "HSM" means an Entrust hardware security module.

1.7. "Hosted Service" means, in this nSaaS Direct Schedule, the nShield as a Service cloud-based platform, including HSMs, which Entrust owns and hosts on its (or its hosting providers') infrastructure.

1.8. "Security World" means the Entrust proprietary protection framework which provides mechanisms to allow keys to be made available for use only by HSMs allocated to the Customer under precisely defined authorization and authentication policies.

1.9. "Self-Managed" means the default nSaaS Direct deployment, where Entrust hosts the Hosted Service, and Customer (i) is responsible for the administration of the Security World; (ii) acts as the Security Officer performing administrative duties requiring Security Officer authorization; and (iii) is responsible for the configuration of the HSMs relevant to the Hosted Service.

1.10. "Service Data" means any information and data relating to the access, use, and/or performance of the Hosted Service, including data generated in connection with Customer's use of the Hosted Service (e.g., analytics data, statistics data and performance data). Service Data does not include Customer Data.

1.11. "SLA" means Entrust's standard service level agreement for the Hosted Service, as may be modified from time to time, as set out in **Attachment 1**.

2. Hosted Service.

2.1. Hosted Service. Customer receives no rights to the Hosted Service other than those specifically granted in this Section 2.1 (*Hosted Service*).

2.1.1. Right to Access and Use. Subject to Customer's compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Service in accordance with: (i) the Documentation; (ii) the information, specifications, and parameters set out in the Customer Enrollment Form; (iii) any specifications or limitations set out in the Order or imposed by technological means on the capabilities of the Hosted Service that Customer is permitted to use; and (iv) and subject to the general restrictions set out in Section 8 of the General Terms (*General Restrictions*).

2.1.2. Service Levels. The sole remedies for any failure of the Hosted Service are listed in the SLA. Service credits issued pursuant to the SLA, if any, will only be applied against the costs associated with Customer's subsequent subscription renewal. Entrust is not required to issue refunds for or to make payments against such service credits under any circumstances.

2.1.3. Service Revisions. Entrust may add, reduce, eliminate, or revise service levels or functionality at any time where a third-party service agreement applicable to the Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice.

2.2. Documentation. Entrust grants Customer a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to use, and create a reasonable number of copies of, the Documentation solely as necessary to support Customer's access to and use of the Hosted Service. Each permitted copy of all or part of the Documentation must include all copyright notices, restricted rights legends, proprietary markings, exactly as they appear on the copy delivered by Entrust or downloaded or otherwise accessed by Customer.

2.3. Support. Entrust provides the support commitments set out in the Support Schedule attached hereto for the Hosted Service.

2.4. Unauthorized Access. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Service or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

2.5. Configuration and Security Measures. Customer is responsible and liable for: (a) account usernames, passwords, and access credentials; (b) the configuration of the Hosted Service to meet its own requirements; (c) Customer Data, Personal Data, and any other data provided to the

Hosted Service by Customer; (d) Customer's access to and use of the Hosted Service; and (e) maintaining adequate security measures and the legally required protection for Customer systems and data in Customer's possession or control or data otherwise residing on Customer systems.

2.6. Customer Roles and Responsibilities. Customer will be responsible for the following with respect to nSaaS Direct (including the Enrollment Services):

2.6.1. Signing and completion of the Customer Enrollment Form;

2.6.2. Identifying for Entrust a primary and alternate points of contact within Customer's organization, as well as additional named point of contacts within the Customer network, cloud, security, and other relevant teams (including, without limitation, as set out in Customer Enrollment Form);

2.6.3. Co-operating with Entrust in all matters, making available to Entrust any information or data as Entrust may reasonably require, and ensuring that all such information or data is complete and accurate in all material respects;

2.6.4. Making available on a timely basis Customer staff with specific knowledge of the nSaaS Direct deployment to engage as required by Entrust staff (e.g. answering technical and other questions, attending meetings, providing sign-off, etc., all within reasonable timeframes);

2.6.5. For a Self-Managed nSaaS Direct deployment, initializing the HSM(s) with the applicable firmware, software (including the Software), and Security World, all as further described in the Documentation, and maintaining control over the applicable administrator card set (ACS);

2.6.6. Maintaining backups of the Customer Data, including key files, stored on Customer's client host(s); and

2.6.7. Purchasing or licensing any Entrust software, smart card readers, or smart cards, as required by Customer's selected deployment (all subject to the relevant separate terms and conditions).

2.7. Enrollment Services. The Customer Enrollment Form shall be (i) signed by Customer prior to Entrust commencing any activities relating to Customer's nSaaS Direct deployment; and (ii) completed by Customer (no later than thirty (30) days following signing) and confirmed by Entrust as further detailed in the Customer Enrollment Form. Any changes to the Customer Enrollment Form initially signed and completed by Customer and confirmed by Entrust, shall be subject to a formal amendment which must be confirmed in writing by Entrust and shall be subject to additional fees. Upon completion of the Customer Enrollment Form, Entrust shall provide the Enrollment Services to Customer to ensure Customer's deployment of nSaaS Direct in accordance with the information, specifications and parameters set out in the Customer Enrollment Form. Such activities shall be subject to the following:

2.7.1. Unless otherwise set out in an Order (and subject to Entrust applicable standard terms and conditions), the provision, installation, and/or configuration of Entrust or third-party hardware, software, operating systems, or supporting network components, are out of scope the Enrollment Services.

2.7.2. nSaaS Direct is subject to the following assumptions and limitations:

2.7.2.1. No visits to Customer premises or other travel are included with the Enrollment Services. Any on premises services would be subject to a separate professional services agreement or statement of work with Entrust;

2.7.2.2. The nSaaS Direct deployment will be implemented and operated using only the HSMs owned and managed by Entrust in authorized Entrust selected data center facilities;

2.7.2.3. Customer will provide its own means of network connectivity via dedicated network connection or Internet Service Provider for access to the data center and service environment;

2.7.2.4. Customer will have facilities to terminate VPN tunnels as specified by Entrust;

2.7.2.5. Customer will perform support, troubleshooting or monitoring of its communications infrastructure and components, network (LAN or WAN) for the purposes of problem resolution; and

2.7.2.6. Network accessibility from Customer sites to external networks or the Internet is outside the scope of nSaaS Direct.

2.7.3. Any deliverables provided by Entrust as part of the Enrollment Services are not “works for hire”. All right, title, and interest in, to and under any intellectual property rights conceived, created, embodied, developed, or reduced to practice by Entrust in the course of providing the Enrollment Services shall vest in and be owned by Entrust and shall be deemed to be the Confidential Information of Entrust. Except as explicitly provided herein, no other license is granted under any intellectual property rights.

2.7.4. Nothing in this Agreement shall prevent Entrust or its Affiliates from providing to a third party the same or similar services as those provided to the Customer as part of the Enrollment Services.

2.8. Customer Default. If Entrust’s performance of any of its obligations in relation to this Agreement is prevented or delayed by any act or omission by the Customer or failure by the Customer to perform any relevant obligations, including, without limitation, those set out in Section 2.6 (*Customer Roles and Responsibilities*) and Section 2.7 (*Enrollment Services*) (each instance a “Customer Default”):

2.8.1.1. without limiting or affecting any other right or remedy available to it, Entrust shall have the right to temporarily suspend performance of the Enrollment Services until the Customer remedies the Customer Default, and to rely on the Customer Default to relieve it from the performance of any of its obligations in each case to the extent the Customer Default prevents or delays the Entrust’s performance of any of its obligations;

2.8.1.2. Entrust shall not be liable for any costs or losses sustained or incurred by the Customer to the extent such costs or losses arise from Customer’s failure or delay to perform any of its obligations as set out herein;

2.8.1.3. reserved;

2.8.1.4. reserved; and

2.8.1.5. reserved.

3. Data and Privacy.

3.1. Customer Data. Customer acknowledges and agrees that the Hosted Service requires certain Customer Data in order to operate. Customer grants to Entrust, its Affiliates, and any of their respective applicable subcontractors and hosting providers, a world-wide, limited right, during the Term, to host, copy, store, transmit, display, view, print or otherwise use Customer Data as reasonably necessary for Entrust (or its Affiliates, and any of their respective applicable subcontractors and hosting providers) to provide the Hosted Service in accordance with the Agreement.

3.2. Service Data. Entrust owns all right, title and interest in and to Service Data and, without limiting the generality of the foregoing, may use, reproduce, or exploit such Service Data in any way, in its sole discretion.

4. **Feedback.**

4.1. Feedback. "Feedback" refers to Customer's suggestions, comments, or other feedback about the Hosted Service or other Entrust products and services. Even if designated as confidential, Feedback will not be subject to any confidentiality obligations binding Entrust. Customer hereby agrees that Entrust will own all Feedback and all associated intellectual property rights in or to Feedback, and Customer hereby assigns to Entrust all of Customer's right, title, and interest thereto, including without limitation intellectual property rights. Entrust acknowledges that the ability to use this Agreement and any Feedback provided as a result of this Agreement in advertising is limited by GSAR 552.203-71.

5. **Warranty Disclaimers.**

5.1. Warranty Disclaimers. For the purposes of this nSaaS Direct Schedule, the following is added to the disclaimer of warranties in the General Terms: Entrust makes no representations, conditions or warranties: (i) that the Hosted Service will be free of harmful components; (ii) that Customer Data and/or Service Data or any other Customer content or data stored in, transferred to or from, or otherwise processed by the Hosted Service, including in transit, will not be damaged, stolen, accessed without authorization, compromised, altered, or lost.

6. **Indemnities**.

6.1. Reserved

7. **Term, Termination and Suspension**.

7.1. Termination or Suspension by Entrust. Entrust may, at its sole discretion, temporarily suspend or Customer's access to the Hosted Service at any time, without advanced notice, if: (i) Entrust reasonably concludes that Customer has conducted itself in a way (a)reserved; or (b) in a way that subjects Entrust to potential liability or interferes with the use of the Hosted Service by other Entrust customers; (ii) Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including, without limitation, the security of other Entrust customers' information or data processed by the Hosted Service; or (iii) Entrust reasonably concludes that Customer is violating applicable laws, rules or regulations. Entrust may also, without notice, suspend Customer's access to the Hosted Service for scheduled or emergency maintenance. Termination of the Agreement will result in termination of all Orders. When the End User is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2. Effect of Termination or Expiry. Without limiting the generality of the effects of termination set out in the General Terms, upon termination or expiry of the Hosted Service, Entrust shall hold the Customer's administrative card sets (ACS) for a period of thirty (30) days following the effective date of termination or expiration; following such time period Entrust shall destroy the ACS and Customer's connection to the Hosted Service, and, at Entrust's sole discretion, destroy, re-allocate, or factory reset the HSMs that were allocated to Customer as part of the Customer's deployment of nSaaS Direct.

Attachment 1

Service Level Agreement (SLA)

1. **Service Levels**.

1.1. **Definitions**. Capitalized terms not defined in this Section (*Definitions*) or otherwise herein have the meanings given to them in the nSaaS Direct Schedule.

1.1.1. "**Downtime**" means, subject to the exclusions below, an interruption of the Hosted Service of five (5) minutes or more during which the ability of ten percent (10%) or more of all users of nSaaS Direct are unable to access the applicable component(s) or function is substantially impaired due to interruptions or impairments. Downtime does not include unavailability resulting from: (i) any Maintenance Windows (as defined below),(ii) suspension or termination of nSaaS Direct in accordance with the terms of the Agreement; (iii) implementation of critical / emergency security patches in accordance with a relevant risk/vulnerability assessment; (iv) factors outside of Entrust's reasonable control, including misconfiguration of Hosted Service by Customer or non-approved changes to the Customer Enrollment Form, as well as any Force Majeure event, Internet accessibility problems beyond Entrust's ISP environment; and (v) issues arising out of Customer's or any third party's network, software, equipment or other technology or service.

1.1.2. "**Maintenance Windows**" are the time frames during which Entrust may perform scheduled routine system maintenance. The Maintenance Windows will not exceed twelve (12) hours per month. Entrust will use commercially reasonable efforts to provide Customer with two (2) weeks' advance notice of the Maintenance Windows.

1.1.3. "**Service Level Credit**" means an amount equal to five percent (5%) of the Monthly Fee for the calendar month in which the Service Level Default (as defined in Section 1.2.2 (*Service Level Credits*)) occurs, where "**Monthly Fee**" means the subscription fees paid to Entrust for nSaaS Direct divided by the number of months in the applicable Term. The total aggregate amount of the Service Level Credit to be issued by Entrust to Customer for all Service Level Defaults that occur in a single calendar month will be capped at five percent (5%) of the Monthly Fee for such calendar month. Service Level Credits can only be applied against the renewal subscription fees due to Entrust for the applicable Offering and any unused Service Level Credits are forfeited upon termination of the Agreement. For clarity, Entrust is not required to issue refunds or make payments against such Service Level Credits under any circumstances, including upon termination of this Agreement. The Service Level Credit is Customer's sole and exclusive remedy for any Service Level Default.

1.1.4. "**Service Level Default**" mean an instance where Entrust has failed to meet any Service Level Target.

1.1.5. "**Uptime**" - is availability of the service calculated in the number of minutes for each year by subtracting the percentage of Downtime (in minutes) during which the service is not available and is calculated as below:

$$\text{Uptime in \%} = \frac{\text{(Availability (in minutes) in Yearly Review Period- Downtime (in minutes))}}{\text{Total minutes in a Yearly Review Period}}$$

1.2. **Targets and Service Level Credits**. The following table describes the service levels for nSaaS Direct:

1.2.1. **Targets** – Entrust will use reasonable commercial efforts to achieve the target set out below:

Offering	Applicable Components/Functions	Target Uptime
nSaaS Direct	HSM cluster availability across two or more datacenters	99.9%
nSaaS Direct	Single instance HSM availability across a datacenter	99%

1.2.2. **Service Level Credits** – In order to receive a Service Level Credit (as defined above), Customer must provide written notice to Entrust within thirty (30) days of the failure if Customer believes there has been a Service Level Default. Upon receipt of such notice, Entrust will verify the accuracy of details provided by Customer against its service logs to determine, acting reasonably, whether a Service Level Default has or has not occurred, and will provide details relating to the cause of the Service Level Default to Customer within thirty (30) days from the date of notification. Customer's failure to provide the notice required in this section will disqualify Customer from receiving a Service Level Credit. Customer will be entitled to receive the Service Level Credit for a confirmed Service Level Default.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the “Support Schedule”), the Entrust General Terms and Conditions (“General Terms”), and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

1.1. “**Business Day**” means any day other than Saturday, Sunday, or a public holiday.

1.2. “**Covered Offering**” means each Hardware, Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support.

1.3. “**Customer-Hosted Offering**” means Hardware, Software, and/or Third Party Vendor Products that are hosted by Customer or installed on Customer’s premises.

1.4. “**Discretionary Extended Support**” means the services which may be available from Entrust under a separate agreement, for End of Support Products or non-standard support relating to reinstatement of Support.

1.5. “**End of Support Product**” means a previous version of Hardware, Software that has entered the End of Support phase as set out in the *Entrust Data Protection Solutions Support Lifecycle Policy* (available upon request), or a Third Party Vendor Product that is no longer supported (as set out in the relevant Documentation for such product).

1.6. “**Hardware**” for the purposes of this Schedule means any “Hardware and Supplies” (as defined in the General Terms) licensed by Entrust under terms attached hereto.

1.7. “**Hosted Service**” for the purposes of this Schedule means nShield as a Service Direct (nSaaS Direct).

1.8. “**Named Support Contacts**” means individual Users nominated by Customer to act as Customer’s support representatives.

1.9. "**Problem**” means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

1.10. “**Production Environment**” means Customer’s live business environment with active users.

1.11. “**Response Time**” means the amount of time that elapses between the Customer’s report of a Service Request to Entrust and Entrust’s acknowledgement of the report, confirmation or assignment of a severity or priority classification, and indicating that a response to the Problem or request has been initiated.

1.12. “**Service Plan**” means the applicable Service Plan for the Covered Offering as referenced in the Support Welcome Pack.

1.13. “**Service Request**” means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

1.14. “**Software**” for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

1.15. "**Support Services**" means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Discretionary Extended Support.

1.16. "**Support Welcome Pack**" means guide to using Support Services for the applicable Covered Offerings containing, inter alia, information related to the relevant Service Plans.

1.17. "**Upgrade**" in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.

2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

4. **Support Fees.**

4.1. Fees for the Support Services will be as set out in the applicable Order in accordance with the GSA Schedule Pricelist and are payable in accordance with the Order and the General Terms.

5. **Customer's Named Support Contacts**.

5.1. When making a Service Request, Customer shall provide:

5.1.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

5.1.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

5.1.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

5.2. For Severity 1 Problems, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Problem. If no dedicated Customer resources are available, Entrust's obligations with respect to the Problem will be suspended until such time as such resources become available.

5.3. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

6. **Support Services For Third Party Vendor Products.**

6.1. Support for Third Party Vendor Products.

6.1.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

6.1.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

6.1.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7. **Upgrades for Customer-Hosted Offerings.**

7.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, and unless otherwise specified, Entrust will have no obligation to provide Support Services for End of Support Products. Entrust may offer to provide Discretionary Extended Support for such End of Support Products for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Discretionary Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

7.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. "for Windows") and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. "for Mac"), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

8. **Exclusions.**

8.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer's failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported Covered Offerings (including, without limitation, End of

Support Products), or (h) with respect to Hardware, an act or omission of Customer related to relocation, movement, or improper installation with reference to the installation Documentation.

8.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer's use of the Covered Offering shall be at Customer's own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

8.3. This Support Schedule expressly excludes on-site support and support for (a) any Covered Offering that was provided on a "no charge", beta testing, proof of concept, evaluation or "not for resale" basis, (b) for hardware other than Hardware, (c) for third party products and services other than Covered Offerings, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

9. <u>**Support Services.**</u>

9.1. **DPS Cloud Security, Encryption and Key Management (formerly "Hytrust") Software**

9.1.1 Help Desk Support. Telephone (+1 (844) 681-8100), email (hytrust.support@entrust.com) and web-based (https://my.hytrust.com) support will be provided to Named Support Contacts (as noted below) between the hours of 5:00 a.m. and 5:00 p.m. Pacific Time, Monday through Friday. Emergency support for Severity 1 Problems will be available twenty-four/seven (24/7/ 365) by contacting: toll-free +1 (844) 681-8100 or creating a Severity 1 case at https://my.hytrust.com. Customer will designate up to three (3) Named Support Contacts and provide their names to Entrust. Only Named Support Contacts may raise a Service Request.

9.1.2 Problem Correction & Service Levels. Each Service Request related to the Software covered by Section 9.1 that has been submitted by Named Support Contact will be issued a tracking number and will be tracked by Entrust. Entrust may acknowledge submission of each Service Request through automated means (e.g. automated response email) or by direct contact via email or phone by an Entrust technical representative within the response times set out below for the applicable severity level. 'Severity Level' is a measure of the relative impact of an issue on Customer's systems or business. Entrust and Named Support Contact will work together to accurately define the severity level for a Service Request.

Severity Level	Impact	Initial Response by Entrust
Severity 1	Software is completely inoperative or at least one component of mission-critical functionality does not perform.	Within one (1) hour. Error diagnosis to commence immediately.
Severity 2	The overall performance of Software is degraded or at least one component of material (but not mission-critical) functionality does not perform.	Within four (4) hours. Error diagnosis to commence immediately.

Severity 3	Any Problem that affects performance of the Software but does not degrade any material or mission critical functionality.	Within twelve (12) hours. Error diagnosis to commence immediately.
Severity 4	General questions, feature requests, etc.	Within twelve (12) hours.

9.1.3 Lapsed Support Services Reinstatement. In the event Support Service expires or is otherwise terminated: (i) any reinstatement of Support Service shall be purchased to cover the lapsed Support Service since expiration or cancelation and must be renewed until the Support Service is current; and (ii) a reinstatement fee of twenty per cent (20%) of the list price shall be charged by Entrust to Customer. In addition, Customer shall warrant that as of the date of the order for renewal is placed that (to the best of its knowledge) all Software covered under this Section 9.1 are functioning correctly. Reinstatement for lapsed Support Services can be backdated to a maximum of eighteen (18) months.

9.1.4 Supported Versions and End Of Life. Unless otherwise specified by Entrust, the provision of Support Services under this Section 9.1 do not apply to End of Support Products. The list of currently supported versions is available on request from the Entrust technical support team.

9.2. **Hosted Service**

9.2.1. Support Services. The availability of Support Services for nSaaS Direct is set out in the Support Welcome Pack available at https://www.entrust.com/-/media/documentation/userguides/dps- nshieldaas-welcome-kit-br.pdf.

9.3. **Hardware Security Modules (nShield HSMs and related Software - excluding products covered under Section 9.1 and 9.2)**

9.3.1. Support Services. The availability of Support Services for Hardware and Software covered under this Section 9.3 is set out in the Support Welcome Pack available at https://www.entrust.com/-/media/documentation/brochures/customer-welcome-pack-technical-support- br.pdf . Entrust will use commercially reasonable efforts to meet the response times noted in the Welcome Pack. Access to the Support Help Center, e-mail or phone lines for the provision of Support may be suspended for brief periods due to scheduled maintenance and other factors. “Support Help Center” means the Entrust nShield Technical Support Help Center that can be accessed from the following link https://www.entrust.com/contact/support.

9.3.2. Lapsed Support Services Reinstatement. In the event Support Service expires or is otherwise terminated: (i) any reinstatement of Support Service shall be purchased to cover the lapsed Support Service since expiration or cancelation and must be renewed until the Support Service is current. In addition, Customer shall warrant that as of the date of the order for renewal is placed that (to the best of its knowledge) all Hardware and Software covered under this Section 9.3 are functioning correctly. Reinstatement for lapsed Support Services can be backdated to a maximum of eighteen (18) months.

9.3.3. Supported Versions and End Of Life. Unless otherwise specified by Entrust, the provision of Support Services under this Section 9.3 do not apply to End of Support Products. The *Entrust Data Protection Solutions Support Lifecycle Policy* defines currently supported versions and is available on request from the Entrust technical support team.

9.3.4. Hardware.

9.3.4.1. Service Plan Options:

9.3.4.1.1. Repair Replacement Option (Standard Support): During an active Support Services term, where the Service Plan purchased by Customer includes the *Repair/Replacement* option, Entrust will repair the original unit or, will ship a replacement unit following receipt of Customer's report and acknowledgement by Entrust that the Hardware in the Order has experienced a Problem which is covered by the Support Services under Section 9.3. Entrust will ship the repaired or replacement unit within fifteen (15) Business Days after receipt at the location specified on the return material authorization ("**RMA**").

9.3.4.1.2. Advance Replacement Option (Premium and Premium Plus Support): During an active Support Services term, where the Service Pan purchased by Customer includes the *Advanced Replacement* option, Entrust will make reasonable efforts to ship a replacement unit by the end of the next Business Day following receipt of Customer's report and acknowledgement by Entrust (report must be received, along with confirmation of Named Support Contact contact details, including name, address, email, and phone number, by 12pm local time for the relevant Entrust support team, failing which the replacement unit will be shipped one the subsequent Business Day – i.e. two Business Days following receipt) that a Product set forth in the Order has experienced a Problem which is covered by Support Services under Section 9.3.

9.3.4.1.3. Rapid Delivery For UK Mainland and On-Site Spare Service Options: During an active Support Services term, where the Service Pan purchased by Customer includes *Rapid Delivery* (available for UK mainland only) or the *On-Site Spare* options, Entrust will, within four (4) operational hours (of a Business Day) of notification that a Hardware unit covered by *Rapid Delivery* support has experienced a Problem and requires replacement, dispatch a support engineer with a replacement Hardware unit. For the *On-Site Spare* option the Customer shall be responsible for holding an additional spare at each of its allocated sites. The Customer is responsible for ensuring that the unit that has experienced a Problem is made available for collection by the support engineer when the replacement Hardware unit is delivered. Customer is responsible for informing Entrust of the location of all units covered by either the *Rapid Delivery* or the *On-Site Spare* option and for informing Entrust of any changes to the locations of the units. Where Customer has used its site Hardware unit spare under the *On-Site Spare* option it shall be accountable for immediately notifying Entrust's technical support team in order that arrangements can be made (with no additional cost to the Customer) to collect the faulty Hardware unit and provision a new Hardware unit that can respectively be stored at Customer's site. The *Rapid Delivery* and *On-Site Spare* options do not include the installation, de-installation or removal of the Hardware units.

9.3.4.2. Hardware Return Material Authorization Policy

9.3.4.2.1. Prior to returning any Hardware to Entrust for repair or replacement, Customer must ensure that: the Hardware is free of any legal obligations or restriction and of any Customer proprietary or confidential information that would prevent Entrust from exchanging, repairing or replacing the Hardware; Customer has obtained a RMA from Entrust, including a RMA number; and it has complied with all applicable export and import control requirements. Certain Hardware components are considered non-returnable items – including, without limitation, smart cards, cables, and rail kits (each "**Non-Returnable Items**"). For a full list of Non-Returnable Items, Customer should contact Entrust technical support prior to the return. Entrust cannot guarantee delivery of any Non-Returnable Items back to the Customer. Export control requirements may require Entrust to provide the full price book value of the Hardware components on Documentation accompanying the RMA shipment.

9.3.4.2.2. All returns must comply with any Entrust RMA instructions set out in the Support Welcome Pack or as advised by Entrust personnel. If Customer does not follow all Entrust RMA instructions, Entrust may invoice Customer the full costs of returning the Hardware.

9.3.4.2.3. Customer shall be responsible for the removal and return of the Hardware that has experienced a Problem and the installation of the replacement Hardware unless the Customer has purchased the *Rapid Delivery* option with respect to such Hardware. Failure to ship the original Hardware back to Entrust within a reasonable period of time following receipt of the replacement Hardware shall cause Customer to be responsible for the retail purchase of the replacement Hardware.

9.3.4.2.4. Reserved.

9.3.4.3. Hardware Upgrades.

Customer recognizes and acknowledges that as a replacement Hardware unit may contain a different or upgraded Software version or other product variants that have developed or evolved over time, a possibility exists that such replacement Hardware unit may not be immediately compatible with Customer's operating environment such as to require Customer to make adjustments to its operating environment.

9.4. **Reserved**.

9.4.1 .

9.5. **Customer Obligations**.

9.5.1. The Customer shall:

9.5.1.1. General.

9.5.1.1.1. Promptly report any identified Problem to Entrust by logging it into the Support Help Center or by email or by telephone as described in the Welcome Pack, documenting it in sufficient detail for Entrust to be able to recreate the Problem, in compliance with its information security responsibilities set forth below, and by providing: Hardware Serial number, a description of the Problem and the circumstances in which it occurred, information on the supported

Hardware and/or Software, e.g. software version, license number, environment etc., diagnostic information (logs, debugs) and an assessment of the severity of the Problem in terms of operational impact;

9.5.1.1.2. Quote the Entrust contract number when reporting the initial problem. Once the Problem has been logged and assigned a ticket number, this number should be quoted in all further communications;

9.5.1.1.3. Use Hardware and/or Software in accordance with the Documentation and promptly and regularly carry out all operator maintenance routines as and where specified;

9.5.1.1.4. Use with Hardware operating supplies and media which comply with Entrust's recommendations;

9.5.1.1.5. Permit only Entrust or Entrust's approved agents to adjust, repair, modify, maintain or enhance the Hardware or Software, save for any operator maintenance specified for Hardware, in which case, permit the Hardware to be used or operated only by properly qualified operators directly under Customer's control;

9.5.1.1.6. Keep adequate back-up copies of the software, data, databases and application programs in accordance with best computing practice. Customer agrees that it is solely responsible for any and all restoration and reconstruction of lost or altered files, data and programs;

9.5.1.1.7. Maintain consistently the environmental conditions recommended by Entrust; and

9.5.1.1.8. Install and implement all solutions, corrections, resolutions, hot fixes and new releases in accordance with Entrust's installation instructions. Customer acknowledges that failure to install such solutions, corrections, resolutions, hot fixes and new releases may cause the Software to become unusable or non-conforming and may cause subsequent corrections and Updates to be unusable. Entrust accepts no liability for the performance of the Software that has not been installed in accordance with Entrust's installation instructions.

9.5.1.2. Access.

9.5.1.2.1. In the event that Entrust agrees to send an engineer to Customer's site, Customer shall permit reasonable access to the Hardware and/or Software for the purpose of carrying out the Support Services and shall make available suitable staff, telecommunications facilities and connections, modem links, electricity, light, heating and other normal services and operating time on any associated system to enable tests to be carried out, including at any remote location if necessary for this purpose. Customer shall provide the Entrust personnel access to the Hardware and/or Software in a place, which conforms to the health and safety regulations of the country where the Entrust personnel is to perform such Support Services.

9.5.1.2.2. Entrust will not require access to any Customer data other than basic contact information from select Customer representatives to provide Support Services and Customer shall take appropriate precautions to prevent transfer of any unnecessary Customer data to Entrust.

10. **Out of Scope Services.** If Customer requires support that goes beyond what is described in this Schedule, including, for example, training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written agreement.

11. **Termination.** In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligations and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate this Support Schedule immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate this Support Schedule in accordance with the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause.

Hardware and Supplies Schedule

If Entrust provides any Hardware and Supplies in connection with an Order, then the following terms apply with respect to the Hardware and Supplies portion of the Offering. Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Shipment; Title and Risk of Loss.** Unless otherwise specified in this Agreement: (i) Hardware and Supplies will be shipped at Entrust's sole discretion either EXW Entrust's dock or FCA Entrust's dock ("INCOTERMS 2020"): (ii) Customer is responsible for obtaining all insurance needed and for all shipping charges; (iii) Hardware and Supplies are deemed to be accepted by the Customer upon delivery in accordance with the INCOTERMS 2020 stated above; and (v) Customer is responsible for installation of the Hardware and Supplies. Legal title and risk of loss of or damage to the Hardware and Supplies pass from Entrust to Customer upon delivery to the shipping carrier in accordance with the applicable INCOTERMS 2020.

2. **Warranties.** Entrust makes no warranties with respect to the Hardware and Supplies or Software associated to Hardware and Supplies other than as set forth in this Schedule or as may be set forth in the documentation delivered by Entrust with the Hardware and Supplies ("Warranty Documentation"), which warranties are subject to the limitations set forth in this paragraph. Entrust warrants that i) Software associated to Hardware and Supplies will perform in accordance with specification set out in the related Documentation for a period of ninety (90) days from the date of delivery; and ii) Hardware and Supplies will be free from defects in material and workmanship for one year unless otherwise set forth in the Warranty Documentation. The remedy for breach of the aforesaid warranty is limited to the repair or replacement of the defective item at no charge to Customer or the refund of the purchase price of the item, at Entrust's sole option, and is conditioned upon (i) Customer's payment of the price or fee specified in an applicable Order (except for purchases via authorized resellers); (ii) the proper use, maintenance, management and supervision of the item; (iii) the exclusive use of Hardware and Supplies or consumable materials supplied by Entrust for the item; (iv) a suitable operating environment for the item; and (v) the absence of any intentional or negligent act or other cause external to the item affecting its operability or performance. This warranty will be null and void if maintenance is performed on a Hardware and Supplies by any party other than Entrust or a qualified party approved by Entrust or if any addition to, removal from or modification of the Hardware and Supplies is made without Entrust's approval. Once they have been replaced, all parts removed from Hardware and Supplies under warranty will become the property of Entrust. If Entrust is requested to provide maintenance service for the Hardware and Supplies that is not covered by the stated warranty, Customer will be responsible for the cost of all such service at Entrust's then-current time and materials rates.

3. **Waste Electrical and Electronic Equipment.** For sales made in the European Union, the Customer alone shall be responsible for, and shall bear the cost of the collection, treatment, recovery and environmentally sound disposal of waste electrical and electronic equipment for the purposes of any decree, statute, regulations, order or other legislation which implements the terms of Directive 2012/19/EU on Waste Electrical and Electronic Equipment in the member state concerned.

4. **Software (and Firmware) License Associated to Hardware and Supplies.** Customer's rights related to Software (and Firmware) Associated to Hardware and Supplies are established by and limited to the terms and conditions specified in the End User License Agreement (EULA) accompanying the Hardware and attached hereto.

5. **Support.** Entrust provides the service levels and Support Services for the Hardware and Supplies (including Software Associated to Hardware and Supplies) as set out in the Support Schedule or a separate Support agreement, a copy of which is available at request. Where Support is purchased

through an authorized reseller and the Order indicates that the reseller will provide Support, such support will be provided by the authorized reseller.

6. **Issuance HSM**. If Customer has purchased an Issuance HSM, Customer is strictly prohibited from using the Issuance HSM as a general purpose HSM and may only use the Issuance HSM for the limited purposes of supporting Entrust's 'Issuance' products. An "Issuance HSM" means a hardware security module ("HSM") that that has been purchased and/or licensed specifically for supporting Entrust's credit card Issuance products.

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope.**

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery**. Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty**.

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination**.

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed

Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users.** Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source.** Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Cryptographic Center of Excellence
PKI Health Check
Schedule

Service Overview
Entrust's Cryptographic Center of Excellence ("CryptoCoE") portfolio of Professional Services Offerings provides the Customer with the consulting services and expertise needed for the Customer to build its own CryptoCoE. Under the PKI Health Check Offering, Entrust will interview key Customer personnel and analyze the Customer's specified governance and system(s) for its public key infrastructure ("PKI") to perform an assessment of PKI solution in place, leading to a report of findings, analysis and recommendations to improve PKI health in the Customer's environment.

The Agreement for the PKI Health Check Offering is made up of this Schedule, the Entrust General Terms and Conditions ("General Terms"), and an Order (as defined in the General Terms) for a PKI Health Check.

1. **Definitions.** Capitalized terms not defined in this Schedule have the meanings given to them in the General Terms.

   1.1. "Expert by Your Side hours" or "EBYS hours" means for the Offering Term, Entrust will provide remote consulting and technical support that is limited to the purchased number of hours in the form of telephone or email assistance (provided during normal business hours), coordinated through an assigned Entrust project manager, to address general inquiries, questions, issues or changes related to the services provided by Entrust.

   1.2. "Technical Account Manager" or "TAM" means a dedicated Technical Account Manager, who is focused on ensuring the Customer's technical product needs are met, while providing escalation support and product roadmap direction.

   1.3. "PKI Governance" means the processes, the policy and organizational structure that the Customer has established to federate its PKI solution.

   1.4. "PKI System" means the technical environment used by the Customer for the PKI solution in place. It includes the servers (physical or virtual), certificate authority software, registration authority software, hardware security modules (HSMs) and associated configurations.

2. **Service Details.**

   2.1. PKI Health Check Subscriptions. If Customer's Order is for a PKI Health Check subscription, Customer will receive the applicable entitlements set out below for the subscription level specified in the applicable Order. Additional PKI environments and Expert By Your Side hours may be purchased as a separate line item on an Order or under an additional Order.

Entitlements	Basic Subscription	Pro Subscription	Premium Subscription
Engagements per Year			
PKI Governance Health Check (see s.2.3)	1	1	1
PKI System Health Check (see s. 2.4)	1	Up to 2	Up to 4
Environments Checked			
PKI System (Root CA)	1	Up to 2	Up to 2
Issuing CAs	Up to 2	Up to 4	Up to 4
Consulting			
TAM	No	No	Yes
Expert By Your Side hours	10	25	50

2.2. One-time PKI Health Check Engagements. If Customer's Order is for a one-time PKI Health Check, Customer will receive the applicable entitlements set out below for the health checks specified in the applicable Order. In the case of a one-time Governance and System Health Check only, additional PKI environments may be purchased as a separate line item on an Order or under an additional Order.

Entitlements	One time PKI Governance and System Health Check	One time PKI Governance Health Check	One time PKI System Health Check
One-time Engagement			
PKI Governance Health Check (see s.2.3)	1	1	none
PKI System Health Check (see s. 2.4)	1	none	1
Environments Checked			
PKI System (Root CA)	1	n/a	1
Issuing CAs	Up to 2	n/a	Up to 2
Consulting	none	none	none

2.3. PKI Governance Health Check

2.3.1. Scope. Entrust will provide a consultant, who will review the Customer's current PKI Governance. The review will be delivered via a sequence of remote meetings. The gathered information will be used to issue at the end of each engagement a detailed report (the "PKI Governance Health Check Report"), as described in Section 3 below. Purchased EBYS hours may be used for remediation of findings.

2.3.2. Stages and Responsibilities. The table below sets out the stages of the PKI Governance Health Check and the respective responsibilities of Entrust and Customer at each stage. The Entrust project manager ("PM") has overall responsibility for ensuring delivery of the

PKI Governance Health Check to the Customer. The PM is the Customer's single point of contact with Entrust for the duration of the engagement, providing co-ordination of resources, tracking and closure of action items, and schedule, requirements and financial management. These steps will be completed for each engagement (the number of engagements depends on what Customer has purchased, as set out in Sections 2.1 and 2.2 above).

Stage	Entrust Responsibilities	Customer Responsibilities
1: Kickoff meeting	• Assign a PM • Explain the process • Schedule the engagement steps and explain dependencies	• Assign a project manager • Engage and manage the required Customer resources • Provide PKI policy documentation (CP, CPS, RPS, PDS) • Provide PKI architecture/design document (if available) or information on the PKI components deployed (CAs, RAs, HSMs, etc). • Identify the policy authority for the PKI
2: Interview Workshop	• Facilitate the workshop • Provide interview questionnaire • Understand the actual Customer process and PKI policy • Review the operational and maintenance processes to ensure that suitable steps are being taken to assure the long-term efficiency of the environments in respect of security, reliability and recovery. • Document the discussion	• Engage stakeholders who are responsible for the organization crypto policy (including policy authority and operational staff)
3: Risk Assessment and Compliancy	• Produce the PKI Governance Health Check Report	• Respond to Entrust's questions
4: Report Presentation	• Meet with Customer to review the PKI Governance Health Check Report and discuss the proposed mitigation/ recommendation plan	• Engage the sponsor team and decision maker

2.4. PKI System Health Check

2.4.1. Scope. Entrust will provide a consultant, who will review the Customer's designated PKI System in order to identify platform issues, readiness to support Customer needs/requirements and proposed improvements. This service can be performed on PKI Systems built on Microsoft Active Directory Certificate Services and/or Entrust PKI software. The gathered information will be used to issue at the end of each engagement a detailed report (the "PKI System Health Check Report"), as described in Section 3 below. EBYS hours may be used for remediation of findings.

2.4.2. Stages and Responsibilities. The table below sets out the stages of the PKI System Health Check and the respective responsibilities of Entrust and Customer at each stage. The Entrust PM has overall responsibility for ensuring delivery of the PKI System Health Check to the Customer. The PM is the Customer's single point of contact with Entrust for the duration of the engagement, providing co-ordination of resources, tracking and closure of action items, and schedule, requirements and financial management. These steps will be completed for each engagement (the number of engagements depends on what Customer has purchased, as set out in Sections 2.1 and 2.2 above).

Stage	Entrust Responsibilities	Customer Responsibilities
1: Kickoff meeting	• Assign a PM • Explain the process • Schedule the engagement steps and explain dependencies	• Assign a project manager • Engage and manage the required Customer resources • Provide PKI architecture/design document (if available) or information on the PKI components deployed (CAs, RAs, HSMs, etc). • Provide PKI policy documentation (CP, CPS, RPS, PDS)
2: Interview Workshop	• Facilitate the workshop • Provide interview questionnaire • Understand the current deployment, business applications and pain points. Clarify where to focus first. • Review the existing deployed infrastructure to establish a clear understanding of the structure of the environment in use including any test and disaster recovery systems. • Request relevant log and configuration files	• Provide the requested log and configuration files • Provide remote access to the platform
3: Risk Assessment and Compliancy	• Asses the current PKI environment usage and compare to the business needs • Check PKI software version and performance • Check the HSM firmware version and log file • Review system logs to identify any outstanding problems or indications of potential future problems • Conduct detailed software assessment of each server within the PKI environment to validate installed versions including patch levels. • Produce the PKI System Health Check Report showing current installation status	• Respond to Entrust's questions
4: Report Presentation and advise	• Meet with Customer to review the PKI System Health Check Report and discuss the proposed mitigation/ recommendation plan	• Engage the sponsor team and decision maker

2.5. Out of Scope. The items below are outside the scope of the PKI Health Check Offering (for clarity, these items are outside the scope of both the PKI Governance Health Check and the PKI System Health Check). Entrust has a rich portfolio of service offerings and could assist the Customer on the tasks below in a separate engagement:

- Provision of any content for policy, procedural or operational documentation.

- Formal project reporting (although informal status reporting will be provided).
- Design, configuration or implementation of any supporting infrastructure for PKI services, for example network design, firewall design or configuration etc.
- Detailed physical implementation of PKI systems, components or infrastructure to support them.
- Legal advice
- Remediation of the findings beyond use of the purchased EBYS hours.
- PKI and/or Crypto Governance consulting
- Travel or any work on Customer's premises

3. **Deliverables**.

3.1. Entrust will provide the following deliverable(s) ("Deliverables") as part of the PKI Health Check Offering, as applicable:

3.1.1. For each PKI Governance Health Check engagement, a PKI Governance Health Check Report comprising:

- Executive summary
- Introduction and background
- Best practices and compliance recommendation
- Grade based on the Customer's adherence to the PKI policy in place
- Highlight issue root cause(s) and recommendation
- Propose policy documentation set and process changes

3.1.2. For each System Health Check engagement, a PKI System Health Check Report comprising:

- Executive summary
- Introduction and background
- High level logical Design
- Confirmation of network connectivity between PKI components
- Highlight all discovered issues, identifying root cause and recommendations
- Recommended configuration changes
- Support status of deployed Entrust products, highlighting where newer versions are available.
- Readiness to support identified expanded or future use cases- roadmap options

3.2. Entrust delivers all documents to its customers in Adobe Acrobat PDF format. This eliminates dependence on a common word processor, provides document integrity and reduces the possibility of transmitting macro viruses to our customers. Upon request, Entrust can also deliver documents in Microsoft Word format.

3.3. Entrust is committed to delivering high quality services and products to its customers. All Deliverables will be subject to peer review and require Entrust Project Manager approval before being delivered to Customer. This also applies to situations where Entrust has chosen to sub-contract certain activities or Deliverables to our partner organizations.

4. **Assumptions and Limitations**.

4.1. Entrust personnel shall not be available or on stand-by for non-Entrust tasks

4.2. All work to be performed during regular business hours.

5. **Fees**. Customer will pay Entrust the costs and fees for the PKI Health Check Offering as set out in the applicable Order in accordance with the GSA Schedule Contract, which are payable in accordance with

the Order and the General Terms.

6. **Warranty**. Entrust warrants that the Professional Services it provides as described in this Schedule shall be performed in a professional manner in keeping with reasonable industry standards.

7. **Term and Termination.**

7.1. The PKI Health Check Offering is sold either as a one-time engagement basis or on a subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for one-time engagements, until the engagement is complete, or (ii) for subscriptions, for a period of one (1) year, in each case, unless terminated in accordance with the Agreement.

7.2. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement with respect to the PKI Health Check Offering and refuse any additional Orders for the PKI Health Check Offering if Customer commits a material breach of this Schedule and fails to remedy such material breach within thirty (30) days after delivery of notice of the occurrence or existence of such breach or such longer period as may be agreed to in writing by Entrust in accordance with the contract Disputes Clause (Contract Disputes Act).

PKI as a Service
Terms of Use

The Agreement for Entrust's PKI as a Service ("PKIaaS") is made up of these terms of use (the "PKIaaS Schedule"), the Entrust General Terms and Conditions ("General Terms") and an Order for PKI as a Service. Capitalized terms not defined herein have the meanings given to them in the General Terms.

You, as the individual accepting the Agreement (as defined in the General Terms), represent and warrant that you are lawfully able to enter into contracts (e.g. you are not a minor). If you are entering into the Agreement on behalf of a legal entity, for example, the company or organization you work for, you represent to us that you have legal authority to bind such legal entity. IF YOU DO NOT ACCEPT THE TERMS AND CONDITIONS OF THE AGREEMENT (OR YOU DO NOT HAVE THE LEGAL AUTHORITY TO ENTER INTO CONTRACTS OR TO BIND THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING SUCH ACCEPTANCE), YOU SHALL NOT ACCESS OR USE THE HOSTED SERVICE. THE CONTINUED RIGHT TO ACCESS AND USE THE HOSTED SERVICE IS CONTINGENT ON CONTINUED COMPLIANCE WITH THE TERMS AND CONDITIONS OF THE AGREEMENT BY YOU (OR BY THE LEGAL ENTITY ON WHOSE BEHALF YOU ARE PROVIDING ACCEPTANCE).

In consideration of the commitments set forth below, the adequacy of which consideration the parties hereby acknowledge, the parties agree as follows.

1. **<u>Definitions</u>**.

1.1. "Administration Information" means information in and related to Management Account and information generated by Customer's usage of the Hosted Service, such as Customer's access credentials, contact information for Administrators, license entitlements, and Certificate consumption.

1.2. "Certificate" means a digital document issued by the certification authority ("CA") that, at a minimum: (a) identifies the CA issuing it, (b) names or otherwise identifies a subject, (c) contains a public key of a key pair, (d) identifies its operational period, (e) contains a serial number and (f) is digitally signed by the CA. Certificates issued by a root CA to an issuing CA are "CA Certificates".

1.3. "CPS" means the most recent version of the Entrust PKIaaS Certification Practices Statement identifying the policy/ies, practices, requirements and rules applicable to the Certificates issued by the Hosted Service attached hereto

1.4. "Customer Content" means any data, text or other content that Customer or any User transfers to Entrust for processing, storage or hosting by the Hosted Service and any computational results that Customer or any User derives from the foregoing through its use of the Hosted Service, and includes Administration Information.

1.5. "Device" means an electronic endpoint in a network, system, or application, such as a computer, laptop, terminal, workstation, server, pager, telephone, smartphone, tablet, microservice container, or other physical object enabled through embedded technology to execute functions and collect and exchange data.

1.6. "Hosted Service" means, in this PKIaaS Schedule, the specific public key infrastructure elements and services of PKIaaS that Customer has purchased as specified in the Order, and includes at a minimum one root CA, one issuing CA, and a Management Account.

1.7. "Management Account" means a self-service administration tool hosted by Entrust that identifies Customer by its full legal name in the "Customer Name" field, tracks Customer's entitlements with respect to the Hosted Service and enables Customer, as applicable in accordance with its entitlements, to manage the issuance, revocation, and expiry of one or more Certificate(s) and provision and configure Hosted Service components and functions.

1.8. "Registration Authority" means a Person responsible for verifying the identity of Subscribers.

1.9. "Relying Party" means a Person that relies on a Certificate and/or any digital signatures verified using that Certificate.

1.10. "Subject" means the Person or Device identified in a Certificate, who or which holds the private key associated with the public key given in the Certificate.

1.11. "Subscriber" means the Person who applies for or is issued a Certificate.

1.12. "User" has the meaning set out in the General Terms, and in this PKIaaS Schedule, includes Customer's Affiliates and any Person who is an Administrator (as defined below), or a Subscriber or Subject of any Certificates issued by the Hosted Service.

2. **PKI as a Service Details**.

2.1. Hosted Service Provision. Entrust will generate, provide and operate, as applicable, the Hosted Service in accordance with the CPS, the Documentation, and Customer's Order(s) for the Hosted Service.

2.2. Security Measures. Entrust will implement and maintain commercially reasonable physical and procedural security controls for the Hosted Service as detailed in the CPS.

2.3. Hosted Service Revisions. Entrust may modify Hosted Service features and functionality at any time. Additionally, Entrust may add, reduce, eliminate or revise service levels at any time where a third-party service level agreement applicable to the Hosted Service has been changed. Where any such change will cause a material detrimental impact on Customer, Entrust will take commercially reasonable efforts to provide Customer sixty (60) days prior written notice (email or posting notice on Entrust's website constitutes written notice). In the event that an Entrust change has a material detrimental impact on the Hosted Service that Customer has purchased, Customer may elect to terminate the affected Hosted Service and Customer shall be entitled to a pro rata refund for any fees pre-paid by Customer for the portion of the affected Hosted Service not yet provided or delivered by Entrust as of the date of termination. It will be Customer's responsibility to notify its Users of any such changes.

3. **Grant of Rights**. Customer receives no rights to the Hosted Service other than those specifically granted in this Section 3 (Grant of Rights).

3.1. General. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to access and use the Hosted Service, and to grant its Users the ability to access and use the Hosted Service, and to distribute Certificates issued by the Hosted Service in each case (a) in accordance with this PKIaaS Schedule and the CPS; (b) in accordance with the Documentation; (b) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Hosted Service that Customer is permitted to use, such as limits associated with subscription levels, on numbers or types of Certificates, identities, Users, signatures or Devices, and on types of deployment (e.g. high availability, test or disaster recovery); and (c) subject to the restrictions set out in Section 3 of the General Terms (Restrictions).

3.2. Evaluation. At Entrust's discretion, it may provide Customer with access to and right to use the Hosted Service for evaluation purposes, in which case, notwithstanding anything to the contrary in the Agreement, either this Section 3.2 (Evaluation) or a separate evaluation agreement executed by the parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms, this PKIaaS Schedule, the CPS, and an applicable Order (if any), for thirty (30) days Customer may, solely as necessary for Customer's evaluation of the Hosted Service, access and use the Hosted Service exclusively in and from a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data). Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 3.1 (General), 7 (Support), 11.1 (Term) and 14 (Publicity) do not apply to any evaluation of the Hosted Service. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Hosted Service at any time, for any or no reason, without advance notice.

4. **Customer Roles and Responsibilities**.

4.1. PKIaaS Participants and Roles. Customer will have one or more roles with respect to the Hosted Service , and will fulfill the responsibilities and functions of such roles as set out in the CPS. In addition, Customer exercises its rights and obligations with respect to the Hosted Service, through individuals that the Customer appoints at its discretion ("Administrators"). The Administrators initially appointed by Customer will be provided to Entrust during enrollment. Such appointment may be modified using means established by Entrust from time to time. Customer agrees that Entrust is entitled to rely on instructions provided by the Administrators with respect to the Hosted Service as if such instructions were provided by the Customer itself.

4.2. Users and Other Third Parties. Customer will make no representations or warranties regarding the Hosted Service or any other matter, to Users, Relying Parties and/or any other third party, for or on behalf of Entrust, and Customer will not create or purport to create any obligations or liabilities on or for Entrust regarding the Hosted Service or any other matter. Entrust may direct any requests or other communications by Users or Relying Parties to Customer.

4.3. Customer-hosted Components. If Customer's Order for a Hosted Service includes on-premise Software components, or if Customer uses any third party products or services in connection with the Hosted Service (collectively, "Customer-hosted Products") Customer will be responsible for the lifecycle management (patching, upgrades, etc.) of such Customer-hosted Products and the security of the environment where it installs and uses such Customer-hosted Products. Customer will implement commercially reasonable security measures with respect to the Customer-hosted Products and the environment where they are installed. Without limiting the foregoing, Customer will: (i) operate the Customer-hosted Products in an environment with appropriate physical, personnel, and electronic security measures; and (ii) for any Customer-hosted Products that are or include software, always use the current version of such software and promptly install any security patches and any upgrades/updates required for proper functioning of all features of the Hosted Service. Customer understands if it fails to comply with this Section it could create a security risk and/or otherwise negatively impact the operation of the Hosted Service and Entrust may have the right to suspend the Hosted Service in accordance with Section 12 (Suspension). In addition, Customer may not be able to access new features or functions of the Hosted Service if it does not comply with this Section.

4.4. Network Requirements. Customer is responsible for procuring, maintaining, monitoring and supporting its communications infrastructure, network (LAN or WAN), and all components that connect to the Hosted Service(s). Entrust assumes no responsibility for the reliability or performance of any connections as described in this paragraph for any such external infrastructure, nor for any service degradation or failures caused by network connectivity of such external infrastructure.

4.5. Devices. For Certificates issued to Devices, Customer is responsible for ensuring that the relevant Devices support and are interoperable with the Certificates.

4.6. Unauthorized Access. Customer will take reasonable steps to prevent unauthorized access to the Hosted Service, including, without limitation, by securing, protecting and maintaining the confidentiality of its access credentials. Customer is responsible for any access and use of the Hosted Services via Customer's Management Account and for all activity that occurs in Customer's Management Account. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Hosted Service or breach of its security and will use best efforts to stop such breach or unauthorized use. The foregoing shall not reduce Customer's liability for all its Users.

5. Customer Content.

5.1. Customer Content and Administration Information. Entrust agrees to access and use the Customer Content only to the extent necessary to provide the Hosted Service, or as necessary to comply with law or a binding order of a governmental body. Notwithstanding the foregoing, the Administration Information may be processed for the purposes of billing, providing Support and to investigate fraud, abuse or violations of this Agreement in the United States, Canada and other locations where Entrust maintains its support and investigation personnel.

5.2. Cloud Risks & Data Safeguards. Customer understands that PKIaaS is a cloud-hosted service. Although Customer Content may be encrypted, Customer acknowledges that there are inherent risks in storing, transferring and otherwise processing data in the cloud, and that Entrust will have no liability to Customer for any unavailability of the Hosted Service, or for any damage, theft, unauthorized access, compromise, alteration, or loss occurring to Customer Content or any data stored in, transferred to or from, or otherwise processed by the Hosted Service, including in transit. Customer is responsible for determining whether the Hosted Service offers appropriate safeguards for Customer's intended use of the Hosted Service, including any safeguards required by applicable laws, prior to transmitting or processing, or prior to permitting Users to transmit or process, any data or communications via the Hosted Service.

5.3. Consents. Customer represents and warrants that Customer (and/or Users) will have obtained any requisite rights and consents, and made any requisite disclosures to relevant Users or other third parties, in accordance with all applicable laws, rules or regulations, to enable Customer and its Users to transfer the Customer Content to Entrust. Customer hereby grants Entrust (including any of its applicable Affiliates, subcontractors or hosting service providers) all rights and consents required for the collection, use, and disclosure of the Customer Content in accordance with the Agreement. Customer shall be responsible for the accuracy, quality and legality of Customer Content and the means by which Customer acquired them.

5.4. Non-Disclosure. For the purposes of this PKIaaS Schedule, the definition of "Confidential Information" in the General Terms excludes any Customer Content. Except as otherwise provided in this Section (Customer Content) or in the Agreement, Entrust shall not disclose to any third party any Customer Content that Entrust obtains in its provision of the Hosted Service. However, Entrust may make such information available (i) to courts, law enforcement agencies or other third parties (including release in response to civil discovery) upon receipt of a court order or subpoena or upon the advice of Entrust's legal counsel, (ii) to law enforcement officials and others for the purpose of investigating suspected fraud, misrepresentation, unauthorized access, or potential illegal activity by Customer in the opinion of Entrust and (iii) to third parties as may be necessary for Entrust to perform its responsibilities under this Agreement.

6. **Software.** If Entrust provides any Software in connection with the Hosted Service, the Schedule provided with the Software will apply (and not this PKIaaS Schedule). If no more specific Schedule is provided with the Software, the Schedule for the Software is the end user license attached hereto.

7. **Support.** Entrust provides the support commitments set out in the Support Schedule attached to this Schedule for the Hosted Service and any Software provided in connection with the Hosted Service. The "Silver Support Plan", as described in the Support Schedule, is included at no additional charge with a subscription to PKIaaS. Other levels of Support may be available for purchase for an additional fee.

8. **Interoperability.** Entrust or third parties may make available plugins, agents or other tools that enable the Hosted Service to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Hosted Service, are licensed separately, and that Entrust grants no rights, warranties or support for any Interoperation Tools or for the interoperability of the Hosted Service with such Interoperation Tools under this PKIaaS Schedule. If Customer uses any Interoperation Tool, Customer has exclusive responsibility to ensure that it has any and all requisite rights to use the Interoperation Tool, including using it to transfer any data from or to the Hosted Service, and to use the product or service with which it connects. The use of an Interoperation Tool does not create any data subprocessor relationship between Entrust and any third party.

9. **Indemnification.**

9.1. Reserved

9.2. Reserved

10. **Fees.** Customer will pay the costs and fees for the Hosted Service as set out in the applicable Order, which are payable in accordance with the Order and the General Terms.

11. **Term & Termination**.

11.1. Term. The Hosted Service is sold on a subscription basis for the Offering Term set out on the Order.

11.2. Termination. In addition to the termination rights in the General Terms, Entrust may terminate the Agreement for the Hosted Service in accordance with the Contracts Disputes Act (i) if Customer commits a material breach of this PKIaaS Schedule and fails to remedy such material breach within 30 days (or such longer period as Entrust may approve in writing) after delivery of the breach notice; and (ii) for any reason by providing Customer advance notice of at least 1 year, unless Entrust discontinues the general commercial availability of the Hosted Service, in which case Entrust may terminate the Agreement upon 180 days' notice to Customer.

11.3. Effects of Termination. Without limiting the generality of the effects of termination set out in the General Terms, upon termination of the Hosted Service, the CAs forming part of the Hosted Service will be inaccessible, Entrust will cease provide status reporting and may revoke the CA Certificates, and Customer's rights to use or access the Hosted Service, including the ability to use the Hosted Service to revoke Certificates, will cease. Customer understands that any use or reliance on unrevoked Certificates is entirely at Customer's own risk.

12. **Suspension**. In the event that Entrust suspects any breach of the Agreement or CPS by Customer and/or Users, Entrust may temporarily suspend Customer's, and/or such Users' access to and use of the Hosted Service without advanced notice, in addition to such other remedies as Entrust may have pursuant to the Agreement. Nothing in the Agreement requires that Entrust take any action against any Customer, User or other third party for violating the Agreement, but Entrust is free to take any such action at its sole discretion.

13. **Open Source Software and Third Party Products**.

13.1. Open Source. Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("**Ancillary Software**"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

13.2. Third Party Products and Services. Certain third-party hardware, software and services may be resold, distributed, provided or otherwise made available by Entrust through or in connection with the Hosted Services ("**Third Party Vendor Products**"). Except as expressly stated in this PKIaaS Schedule, Entrust has no obligation and excludes all liability with respect to Third Party Vendor Products, the use of which shall be exclusively subject to the third party vendor's terms, conditions and policy documents ("**Vendor Terms**") accompanying, embedded in, or delivered with the Third Party Vendor Products, or otherwise made available by the third party vendor. In particular,

13.2.1. If Customer purchases any Sixscape products (e.g. SixMail, SixEscrow) through Entrust or in connection with PKIaaS, use of the Sixscape products shall be subject to the SixScape Vendor Terms embedded in or delivered with the products and those which can be retrieved at www.sixscape.com/product-and-warranty. Entrust shall provide support in relation to the Sixscape products pursuant to the Support Schedule attached hereto.

14. **Publicity**. During the Term and for thirty (30) days thereafter, Customer grants Entrust the right, free of charge, to use Customer's name to identify Customer as such on Entrust's website or other marketing or advertising materials to the extent permitted by the General Services Acquisition Regulation (GSAR) 552.203-71.

Entrust End User License

If Entrust provides any Software to Customer, alone or in connection with any other type of Offering (e.g. a Hosted Service), and no separate license was provided with such Software, the Agreement for the Software is comprised of this end user license ("Software Schedule"), the Entrust General Terms and Conditions ("General Terms"), and an Order for the Software (or for the Offering in connection with which the Software is provided). Capitalized terms not defined herein have the meanings given to them in the General Terms.

1. **Scope**.

1.1. The Software and related Documentation is protected by copyright and other intellectual property laws and treaties. Copies of the Software and related Documentation provided to Customer (or Users) pursuant to the Agreement are licensed, not sold, and neither Customer nor any User receives any title to or ownership of any copy of the Software and/ or Documentation itself.

1.2. This Software Schedule, on its own, does not grant any entitlement to receive any Support or upgrades to the Software. If Customer is entitled to receive Support for the Software, for example if the Order for the Software indicates that Support is included with the Software or has been purchased separately for the Software, then such support will be provided pursuant to the then-current applicable Support Schedule. The Software includes any upgrades to which the Customer is entitled, subject to additional terms (if any) that may be applicable to the enhanced features made available as part of the upgrade.

1.3. Interoperability. Entrust or third parties may make available plugins, agents, or other tools that enable the Software to interoperate with third party products or services (each, an "Interoperation Tool"). Customer acknowledges and agrees that such Interoperation Tools are not part of the Software. Except for Interoperation Tools expressly licensed by Entrust under this Software Schedule, Entrust grants no rights, warranties or support for any Interoperation Tools hereunder.

2. **Grant of Rights.**

2.1. Customer receives no rights to the Software and Documentation other than those specifically granted in this Section 2 (Grant of Rights).

2.2. General License Grant. Subject to Customer's (and Users') compliance with the Agreement, Entrust grants Customer, during the Offering Term, a personal, worldwide, non-exclusive, non-transferable, non-sub-licensable right to: install and use the Software and use the Documentation, and to grant its Users the ability to access and use such Software and Documentation, in each case (a) in accordance with this Software Schedule; (b) in accordance with the Documentation; (c) in accordance with any specifications or limitations set out in the Order or imposed by technological means (such as a license code provided by Entrust) of the capabilities of the Software that Customer is permitted to use, such as limits associated with subscription levels, on copies of Software, on numbers or types of certificates, identities, users, signatures, protocols or devices, and on types of deployment (e.g. high availability, test or disaster recovery); (d) with respect to Software embedded in Hardware and Supplies, only on the Hardware and Supplies on which the Software is installed (and not separately or apart from such Hardware and Supplies); (e) only on the operating systems or technology platforms designated by Entrust; (f) for internal business purposes only, unless specifically authorized by Entrust in the Documentation, Order, or otherwise; and (g) subject to the general restrictions set out in Section 3.1 of the General Terms (General Restrictions).

2.3. Evaluation. At Entrust's discretion, it may provide Customer with access to and the right to use the Software for evaluation purposes, in which case and notwithstanding anything to the contrary in the Agreement, either this Section (Evaluation) or a separate evaluation agreement executed by both parties will apply. Subject to Customer's compliance with all restrictions, conditions and obligations in the General Terms and this Software Schedule, for thirty (30) days Customer may solely as necessary for Customer's evaluation of the Software install and use the Software exclusively in a test (non-production) environment (and which environment contains, for clarity, only fictitious non-production data) in such quantities, and subject to any restrictions on uses, as specified by Entrust. Entrust may extend the evaluation period in writing at its discretion. Evaluation purposes exclude any purpose from which Customer (or any of its Users) generates revenue. Sections 2.2 (General License Grant), 6 (Warranty), 7.1 (Term), and 10 (Publicity) of this Software Schedule do not apply to any evaluation of the Software. Entrust may in its sole discretion suspend or terminate any and all evaluation access and other evaluation rights to the Software at any time, for any or no reason, without advance notice.

3. **Delivery.** Entrust shall make the Software available for electronic download subject to the receipt of all required documentation, including any required export and import permits. Thereafter, Customer shall be responsible for making the permitted number of copies and distributing such copies if and as permitted in the Agreement. Customer will be the importer of record for the Software.

4. **Installation and Management.** Except for any installation Professional Services to be performed by Entrust pursuant to an Order, Customer agrees that it will be responsible for installing and managing the Software in accordance with the Documentation. Entrust will have no responsibility or liability for any impact to or failure of the Software or any Offering with which the Software was provided resulting from Customer's (or Users') improper installation and/or management of the Software.

5. **Audit Rights.** Customer shall keep reasonable records relating to Customer's use of the Software sufficient to show compliance with the Agreement ("Usage Records"). A chartered or certified public accountant selected by Entrust may, upon reasonable notice and during normal business hours, but no more often than once a year, inspect such Usage Records. If the audit reveals that Customer's use has not been been in compliance with the Agreement and as a result has not paid the full or correct price for its actual use, Entrust may invoice the unpaid price based on the GSA Schedule price list current at the time of the audit.

6. **Warranty.**

6.1. Software Warranty. Entrust warrants that (i) for a period of ninety (90) days from the date of delivery each item of Software will perform in substantial accordance with the Documentation, as applicable to the scope of license purchased by Customer as set out in the Order; and (ii) at the time of delivery, Entrust shall have used commercially reasonable efforts to cause the Software to be free of any known computer virus or harmful, malicious, or hidden software, data, or other computer instructions whose purpose is to disrupt, damage, or interfere with the licensed use of computer and telecommunications software or hardware for their normal purposes ("Malware").

6.2. Warranty Exclusions. The warranty in Section 6.1 (Software Warranty) shall not cover or apply with respect to any damages, malfunctions or non-conformities caused by (i) failure to use the Software in accordance with the Agreement and the Documentation; (ii) accident, misuse, abuse, improper operation, installation, misapplication, or any other cause external to the Software; or (iii) any modifications or additions made to the Software by Customer or by a third party acting for the

Customer.

6.3. Remedy for Breach of Warranty. Entrust's exclusive liability and the Customer's sole and exclusive remedy for breach of the provisions of this Section (Warranty) shall be, at Entrust's option, to correct, repair or replace, free of charge, the Software which does not meet Entrust's warranty.

7. **Term and Termination**.

7.1. Term. The Software may be licensed on a perpetual or subscription basis, as specified in the Order. Unless otherwise specified on the Order, the Offering Term will commence on the date that the Order is accepted by Entrust and will continue in effect either (i) for perpetually-licensed Software, for so long as Customer continues to use the Software, or (ii) for subscription Software, for a period of one (1) year or such other period as stated in the Order, in each case, unless terminated earlier in accordance with the Agreement.

7.2. Termination. In addition to the termination rights in the General Terms:

7.2.1. When the Customer is an instrumentality of the U.S., recourse against the United States for any alleged breach of this Agreement must be brought as a dispute under the contract Disputes Clause (Contract Disputes Act). During any dispute under the Disputes Clause, Entrust shall proceed diligently with performance of this Agreement, pending final resolution of any request for relief, claim, appeal, or action arising under the Agreement, and comply with any decision of the Contracting Officer.

7.2.2. Customer may terminate a perpetual license to Software granted under this Software Schedule by destroying all copies of the Software under its control and notifying Entrust of such destruction.

8. **U.S. Government End-Users**. Any software and documentation provided under the Agreement are commercial items, as that term is defined in 48 CFR 2.101, consisting of commercial computer software and commercial computer software documentation, as those terms are used in 48 CFR 12.212. If software or documentation is acquired by or on behalf of the U.S. government or by a U.S. government contractor (including without limitation prime contractors and subcontractors at any tier), then in accordance with 48 CFR 12.212 (for licenses with all federal government agencies), the government's rights to such software and documentation are limited to the commercial rights specifically granted in the Agreement, as restricted by the Agreement. The rights limited by the preceding sentence include any rights to reproduce, modify, perform, display, disclose, release, or otherwise use the software or documentation. This Section (U.S. Government End-Users) does not grant Customer any rights not specifically set forth in the Agreement. Customer shall not remove or deface any restricted rights notice or other legal notice appearing in any software or documentation or on any associated packaging or other media. Customer shall require that its U.S. government users of any software or documentation agree to and acknowledge the provisions of this Section (U.S. Government End-Users) in writing.

9. **Open Source.** Versions of certain third-party open source software (including libraries and redistributable files) may be embedded in, delivered with or automatically downloaded as part of any Software ("Ancillary Software"). The Ancillary Software is subject to the applicable separate open source license agreement(s) pertaining to the Ancillary Software, which shall be provided with the Software or otherwise made available by Entrust. The complete list of Ancillary Software (not the Ancillary Software itself) shall be deemed Entrust Confidential Information.

Support Schedule

The Agreement for any Support provided with respect to Covered Offerings (defined below) is made up of these Support terms (the “Support Schedule”), the Entrust General Terms and Conditions (“General Terms”)**,** and an Order for such Support. Capitalized terms not defined herein have the meanings given to them in the General Terms or the applicable Covered Offering Schedule.

1. **Definitions.** The following terms shall have the meaning ascribed to them as follows:

   1.1. “**Business Day**” means any means any day other than a Saturday or Sunday. For greater certainty, an event occurring outside of the hours between 8:00AM to 8:00PM Eastern Standard Time (EST) will be deemed to have occurred at the start of the next Business Day.
   1.2. “**Covered Offering**” means each Hosted Service, Software, and Third Party Vendor Product for which Entrust provides Support Services.
   1.3. “**Customer-Hosted Offering**” means Software and/or Third Party Vendor Products that are hosted by Customer or installed on Customer’s premises.
   1.4. “**Extended Support**” means the services which may be available from Entrust under a separate agreement, for Superseded Products or non-standard support relating to reinstatement of Support Services.
   1.5. “**Hosted Service**” for the purposes of this Schedule means Entrust’s Identity as a Service, Certificate Services, Signing Automation Service, Remote Signing Service, PKI as a Service, Managed PKI, Managed Certificate Hub, Cryptography as a Service, Managed Root CA, and/or Managed Microsoft PKI.
   1.6. “**Incident**” means a Service Request that has been classified as Severity 1 in accordance with this Schedule.
   1.7. “**Named Support Contacts**” means individual Users nominated by Customer to act as Customer’s support representatives.

   1.8. "**Problem**” means a reproducible defect that causes the Covered Offering to fail to conform to its applicable current Documentation.

   1.9. “**Production Environment**” means Customer’s live business environment with active users.

   1.10. “**Response Time**” means the amount of time that elapses between the Customer’s report of a Service Request to Entrust and Entrust’s acknowledgement of the report, confirmation or assignment of a severity classification, and indicating that a response to the Problem or request has been initiated.

   1.11. “**Service Plan**” means either; (i) the **Silver Service Plan**, or (ii) the **Platinum Service Plan**, as set out in Section 8.

   1.12. "**Service Request**” means a reported Problem or request specific to a Covered Offering which is unique from any other opened support cases reported by Customer.

   1.13. “**Software**” for the purposes of this Schedule means any Software (as defined in the General Terms) licensed by Entrust under terms that incorporate this Schedule by reference.

   1.14. “**Superseded Product**” means previous version(s) of the Software or Third Party Vendor Product(s).

   1.15. “**Support Services**” means the services described in this Support Schedule relating to the Covered Offerings that are provided by Entrust according to the Service Plan specified in the applicable Order, and excludes Extended Support.

   1.16. “**Upgrade**” in the context of Software and Third Party Vendor Products that are commercial software products, means a subsequent release or version of the Software/Third Party Vendor Product; Upgrade releases will be designated by a change in the release number.
2. **Support Provision.** Entrust will provide the Support Services in accordance with the applicable Service Plan set out in the Order.

3. **Additional Benefits.** Customers who have purchased a Platinum Service Plan may be entitled to receive certain additional benefits relating to the specific type of Covered Offering that they have purchased, as set out in the Platinum Service Plan Documentation.

4. **Support Term.** The Offering Term for Support Services is as set out in the applicable Order, or, if not specified in the applicable Order, is for a period of twelve (12) months.

5. **Support Fees.**

5.1. Any and all fees for the Support Services will be as set out in the applicable Order and are payable in accordance with the Order and the General Terms.

5.2. Customer may reinstate lapsed Support Services for any currently-supported version of the Software by paying all support fees in arrears to a maximum of thirty-six (36) months. Notwithstanding the foregoing, to the extent Entrust reasonably determines that reinstatement of Support Services would require non-standard assistance (e.g. as a result of issues excluded from the scope of this Schedule), such support shall be considered Extended Support.

6. **Customer's Responsibilities**.

6.1. For Customer-Hosted Offerings, Customer shall establish proper backup procedures, in accordance with the process Documentation provided by Entrust, necessary to (i) replace critical data in the event of loss or damage to such data from any cause, (ii) recover the system in the event of error, defect or malfunction.

6.2. Customer will be responsible for nominating Named Support Contacts up to the maximum number permitted under the applicable Service Plan. The Named Support Contacts will be registered in Entrust's systems in association with Customer's account, and Customer may update its Named Support Contacts from time to time. Customer shall ensure that its Named Support Contacts are educated and trained in the proper use of the Covered Offerings in accordance with applicable Documentation.

6.3. Customer, through its Named Support Contacts, will be responsible for providing First Line Support to Customer's Users of the Covered Offerings. "First Line Support" means the provision of a direct response to all of Customer's Users with respect to inquiries concerning the performance, functionality or operation of the Covered Offerings; initial diagnosis and trouble-shooting of Problems with the Covered Offerings; and addressing inquiries and Problems reasonably solvable with reference to the associated Documentation for the Covered Offerings. If, after commercially reasonable efforts, Customer is unable to answer, diagnose or resolve Problems with the Covered Offerings, one of the Named Support Contacts may contact Entrust to make a Service Request. Further, if Customer believes an Service Request may be a Severity 1 Incident, it must make the Service Request by telephone.

6.4. When making a Service Request, Customer shall provide:

6.4.1. All relevant system configuration settings, and keep Entrust informed of any relevant changes made to it. Customer is responsible for re-validating any configuration settings prior to moving to a Production Environment.

6.4.2. Access to qualified functional or technical personnel to aid in diagnosis and to assist in repair or remediation of any Problem reported in the Service Request

6.4.3. Upon Entrust's request, additional data deemed necessary or desirable by Entrust to reproduce the environment in which a reported Problem occurred, or to otherwise address the Service Request.

6.5. For Severity 1 Incidents, Customer must have dedicated resources available to work on the issue on an ongoing basis during the reported Incident. If no dedicated Customer resources are available, Entrust's obligations with respect to the Incident will be suspended until such time as such resources become available.

6.6. Unless specifically permitted in the applicable Agreement, Customer (and its Named Support Contacts) shall only contact Entrust, and not any of its suppliers or licensors, with questions or Problems relating to the Covered Offerings.

7. **Support Services.** Support Services include the following services:

7.1. Entrust Support Portal. Entrust makes available a support portal which is accessible 24 hours a day, 7 days a week except for any downtime experienced due to periodic maintenance or network unavailability, which if scheduled, will occur on the weekend. Notice of any scheduled downtime is provided on the portal. Customer may use the portal to:

7.1.1. access and view Documentation for the Covered Offerings, support knowledge base, the Entrust support newsletter, Software lifecycle information, and security bulletins;

7.1.2. download (where applicable) Covered Offerings; and

7.1.3. log, view and receive updates on Customer's Service Requests.

7.2. Entrust will provide Second Line Support for the Covered Offerings, which will be available by telephone, chat and email. "Second Line Support" means (i) communicating with Customer's Named Support Contacts with respect to Service Requests; (ii) diagnosis of Problems reported in Service Requests; (iii) addressing Problems reported in Service Requests to the extent that they are within Entrust's control. The availability of Second Line Support is set out in the applicable Service Plan. With respect to suspected Severity 1 Incidents reported by telephone, if the call is not immediately answered, and Customer leaves a voicemail reporting a suspected Severity 1 Incident, Entrust shall use commercially reasonable efforts to acknowledge and confirm the classification within one (1) hour of receipt of the voicemail ("Immediate Incident Response Time").

7.3. Support for Third Party Vendor Products.

7.3.1. If Entrust provides Support Services for any Third Party Vendor Product, as specified in an Offering Schedule, Order, or as agreed by the parties in writing, Entrust will use commercially reasonable efforts to support such Third Party Vendor Product in the same manner as other Covered Offerings, with the following exceptions: (a) if resolution of any Service Request requires changes or fixes to the Third Party Vendor Product or other assistance from the third party vendor, Entrust's sole obligation will be to escalate such Service Request to the applicable vendor; and (b) any time periods set out in this Schedule shall exclude any time during which Entrust is required to wait for a response or resolution from the vendor.

7.3.2. Customer will be responsible for testing any changes or fixes provided by the vendor to fix any Problems relating to a Third Party Vendor Product and notify Entrust if any additional issues or deficiencies are identified or if the change or fix does not resolve the Problem (or creates a new one).

7.3.3. Unless otherwise agreed by the parties in writing, Customer will not contact the vendor of any Third Party Vendor Product directly, but instead will communicate any Service Requests to Entrust.

7.4. Service Request Classification. When Customer makes a Service Request, Entrust will, in consultation with Customer, first classify the Service Request according to its severity and nature. The Service Request will then be logged in Entrust's Service Request tracking system and classified into one of the following categories below. If Customer believes a Service Request may be a Severity 1 Incident, it must report the Incident by telephone.

Severity 1	Production server or other mission critical system(s) are down and no workaround is immediately available.
Severity 2	Major functionality is impacted or significant performance degradation is experienced. The situation is causing a high impact to portions of Customer's business operations and no reasonable workaround exists.
Severity 3	Inquiry regarding a routine technical issue; information requested on application capabilities, navigation, installation or configuration; bug affecting low number of users or an acceptable workaround is available.

7.5. Responding to Reported Service Request. Service Request will be handled according to their level of severity in the manner set out below:

7.5.1. Severity 1 Incidents - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 1 Incident within the target Response Times set out in the applicable Service Plan. The resolution and correction of Severity 1 Incidents may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.2. Severity 2 Service Requests - Entrust shall promptly initiate and continue diagnostic and remedial measures, using qualified employees and in a workmanlike manner conforming to standards generally accepted in the software support industry. Entrust shall make commercially reasonable efforts to respond to a Severity 2 Service Request within the timeframes set out in the applicable Service Plan. The resolution and correction of Severity 2 Service Requests may be implemented through a work-around, software fix, web interface fix or upgrade.

7.5.3. For Severity 1 Incidents and Severity 2 Service Requests, Entrust shall advise Customer periodically at reasonable intervals as to the progress made by Entrust in diagnosing and/or correcting any reported Incident.

7.5.4. In the event of a Severity 3 Service Request for a Problem, Entrust may include the resolution in the next infrastructure software upgrade or web interface upgrade.

7.6. Service Plan. The following table describes the service levels for the Silver Service Plan and Platinum Service Plan:

Support Service	**Silver Service Plan**	**Platinum Service Plan**
Maximum number of Named Support Contacts	5	10
Availability of technical support services by telephone	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time)	24/7/365
Priority telephone call handling:	No	Yes
Availability of technical support services by email/chat	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)	24/5 (Sunday, 20:00 Eastern time to Friday, 20:00 Eastern time, except for December 25)
Priority email handling:	No	Yes
Immediate Incident Response Time	1 hour	1 hour
Call back for voicemail (Except for calls reporting Severity 1 Incidents)	24 Hours	24 Hours
Response Time target for reported Service Requests		
Severity 1 Incidents	8 hours	4 hours
Severity 2 Service Requests	2 Business Days	1 Business Day
Severity 3 Service Requests	3 Business Days	2 Business Days

8. **Upgrades for Customer-Hosted Offerings**.

   8.1. Software Upgrades. Entrust will use commercially reasonable efforts to make available to Customer all Upgrades for Software and Third Party Vendor Products generally available from Entrust at no additional cost to Customer. Upon the release of each Upgrade, Entrust will have no obligation to provide Support Services for Superseded Products. Entrust may offer to provide Extended Support for such Superseded Product for an additional charge under the terms and conditions of a separate agreement. If Customer is interested in purchasing Extended Support, Customer may contact an Entrust sales representative or authorized reseller for more information.

   8.2. Platform Options. If Customer has licensed a platform-specific version of Software (server Software only, e.g. “for Windows”) and Entrust also offers the same version of the Software on an Entrust-supported computing platform other than the platform on which Customer originally licensed such Software (e.g. “for Mac”), upon request, Entrust will, at no additional charge, other than shipping costs, provide Customer with a copy of the alternate platform version of the Software as a replacement for the originally-licensed version. Customer may use the alternate platform version of the Software for the new platform pursuant to the same terms and conditions applicable to the original platform version of the Software, provided that Customer may not run both versions of the Software concurrently.

9. **Exclusions**.

   9.1. Entrust shall have no obligation to provide Support Services under this Support Schedule if a Service Request is made because of: (a) Customer’s failure to maintain proper site or environmental conditions, (b) any fault of Customer or any User, including misconfiguration of components, improper use, or use that is not in accordance with the applicable Documentation, (c) any attempts at repairs, maintenance, or modifications to the Covered Offerings performed by a Person other than authorized service personnel of Entrust, (d) the acts of third parties (unless authorized by Entrust), (e) failure or interruption of any electrical power, telephone or communication line or like cause, (f) Problems caused by third party software, hardware or services, including but not limited to web server and web browser software, plug-ins and integrations, or (g) use of unsupported software (including Superseded Products).

   9.2. If Entrust recommends having a Covered Offering deployed in a test environment prior to deployment in a Production Environment, and Customer chooses not to follow such advice, then Customer’s use of the Covered Offering shall be at Customer’s own risk and any Service Requests relating to such Covered Offering will be classified and treated as if they were in a test environment.

   9.3. This Support Schedule expressly excludes on-site support and support for (a) any Offering that was provided on a “no charge”, beta testing, proof of concept, evaluation or “not for resale” basis, (b) for Hardware, (c) for third party products and services other than Third Party Vendor Products as defined herein, including for applications that utilize Entrust toolkit software products, and (d) for non-Entrust developed integrations of the Covered Offerings with third party products or services.

10. **Out of Scope Services**. If Customer requires support that goes beyond what is described in this Schedule, including for example training and on-site services, such services may be available for purchase from Entrust pursuant to a separate written Agreement.

11. **Termination**. In addition to the termination rights in the General Terms, if either party is in material breach, or fails to perform one or more of its material obligations under this Support Schedule, the other party may, by written notice to the party in material breach, require the remedy of the material breach or the performance of the material obligation and, if the party so notified fails to remedy or produce a reasonable plan to remedy (which if such plan is not followed by the breaching party shall entitle the other party to terminate the Agreement for Support immediately), or perform within thirty (30) days of the written notice, declare the party in material breach to be in default and terminate the Agreement for Support in accordance with the contract Disputes Clause (Contract Disputes Act).