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") provided with this ECSS Schedule and which are also available at https://www.entrust.com/-/media/documentation/licensingandagreements/repository-general-terms.pdf, 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 available at https://www.entrust.com/end-user-license.pdf (and not this ECSS Schedule).

8. **Support Services**. Entrust provides the support commitments set out in the Support Schedule available at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf 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. Additional Customer Data and Use Claims. In addition to Customer's indemnification obligations in Section 10.2 (Customer Data and Use Claims) of the General Terms, Customer shall defend, indemnify and hold harmless Entrust, its Affiliates and licensors and each of their respective employees, officers, directors, and representatives against any and all third party claims, demands, suits or proceedings, fines, costs, damages, losses, settlement fees, and expenses (including investigation costs and attorney fees and disbursements) arising out of or related to: (a) Customer's breach of, or errors in providing, the representations and warranties set out in Section 6.6 (Consents); (b) a violation of applicable law by Customer, Users, or Cloud Content; (c) an allegation that the Cloud Content infringes or misappropriates a third party's intellectual property rights; and (d) a dispute between Customer and any User (each of (a)-(d) are deemed included in the definition of "Customer Indemnified Claim" in the General Terms).

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. Non-payment of Fees. If payment is not received within ten (10) business days of written notice that a payment is delinquent, Entrust may, in addition to the rights set out in the General Terms, revoke all Certificates.

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 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 its discretion with notice to Customer 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. In the event that Entrust suspects any breach of the Agreement or the CPS by Customer and/or Users, Entrust may suspend Customer's and/or such Users' access to and use of the Hosted Services without advance 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.

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 CLICKING THE "ACCEPT" ICON BELOW 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 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 available at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf.

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. **Third Party Beneficiaries**. Customer is notified that there are third-party beneficiaries to the Agreement. The Certificate Beneficiaries are expressly agreed to be third party beneficiaries under the Agreement for Certificate Services. In addition, with respect to the provisions of the Agreement that relate to (i) use of certain components of an Offering in which such third parties have an interest, (ii) products and services provided by third party subcontractors, suppliers and licensors of Entrust, or (iii) Third Party Vendor Products provided by third party vendors; such provisions are made expressly for the benefit of such third-party beneficiaries and are enforceable by such third-party beneficiaries in addition to being enforceable by Entrust.

19. **Publicity.** 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 a customer on Entrust's website or other marketing or advertising materials.

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 available at https://www.entrust.com/-/media/documentation/whitepapers/code-signing-best-practices-v2.pdf 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.