Terms of Use

Entrust's Certificate Services, Certificate-based Signing Services, Time-stamping Services and/or Dedicated CAs are subject to these Offering-specific terms of use (this "Schedule") and the Entrust General Terms and Conditions ("General Terms") provided with this Schedule and which are also available at https://www.entrust.com/general-terms.pdf. Certificates are also subject to Subscriber Agreements (as defined below). 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. "**CA**" means the system that issues and signs Certificates and the certification authority entity that operates such system.

1.2. "**Certificate**" means a digital document 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.

1.3. "**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.

1.4. "**Dedicated CA**" means an issuing CA chaining up to a public root CA and dedicated to issuing Certificates for Customer.

1.5. "**Documentation**" has the meaning set out in the General Terms, and in this Schedule, includes the Policy and Practices Documentation.

1.6. "**Enterprise RA**" means an employee or agent of a Subscriber who acts as an RA solely for that Subscriber.

1.7. "**Foreign Certificate(s)**" means any Certificate that was not issued to or for Customer using its Management Account. For greater certainty, Foreign Certificates may include, but are not limited to, Certificates issued from other management services accounts, Certificates purchased from third parties, and Certificates issued from other Entrust service offerings (for example, PKI as a Service).

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 Schedule, the specific Certificate Services, 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 industry or regulatory standards or requirements applicable to a particular Certificate or Time-stamp, as identified in the Policy and Practices Documentation.

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 Time-stamping Services and Signing Services.

1.12. "**Policy and Practices Documentation**" means, collectively, the most recent versions of the policy/ies, practices, requirements and rules applicable to a Certificate or Time-stamp provided by Entrust, and the practices statements applicable to public key infrastructure (PKI) or components thereof operated as part of a Hosted Service, all as posted in Entrust's repository at http://www.entrust.net/cps, as may be amended from time to time. The Policy and Practices Documentation applicable to a specific Certificate, Time-stamp and/or PKI depends on the type and nature of the Certificate, Time-stamp and of the PKI.

1.13. "**RA**" means a registration authority authorized by a CA to carry out certain verification tasks for Certificates as set out in applicable Policy and Practices Documentation.

1.14. **"Signing Services"** means the services offered by Entrust relating to the generation, management and hosting of key pairs used to apply Certificate-based signatures and seals to hashed data.

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

1.16. "**Subscriber**" means the Person who applies for or is issued a Certificate or a Time-stamp.

1.17. "**Subscriber Agreement**" means the agreement or terms of use posted in Entrust's repository at http://www.entrust.net/cps applicable to a particular Certificate type, between the CA who issues such Certificate and the Subscriber (and the Subject, if applicable).

1.18. "**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.

1.19. "**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.

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

2. Hosted Services Details. Entrust will provide the Hosted Services in accordance with the applicable Documentation and Customer's Order(s) for the Hosted Services. Without limiting the foregoing:

2.1. Certificate Services—Verification, Issuance and Revocation of Certificate(s). Upon receipt of an application containing requisite Subscriber and Subject information, and subject to the Subscriber's acceptance of the Subscriber Agreement, one or more RAs will perform verification as described in the Policy and Practices Documentation and Subscriber Agreement for the applicable type of Certificate(s). Subject to successful verification, upon receipt of a Certificate issuance request, the applicable CA will issue the Certificate(s) as described in the Policy and Practices Documentation and Subscriber Agreement for the applicable type of Certificate(s). After issuance, Entrust will make the Certificate(s) available for retrieval and management as set out in the Documentation and Customer's entitlements under its Order for Certificate Services. **Customer acknowledges and agrees that Certificates are subject to revocation as set out in the applicable Subscriber Agreement, which may require revocation within a matter of hours or days, depending on the circumstances and that it is each Subscriber's responsibility to ensure it is able to safely replace a Certificate in case it needs to be revoked within 24 hours.**

2.2. 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 Documentation and Customer's entitlements under its Order for Signing Services.

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

2.4. Dedicated CA. If an Order calls for one or more Dedicated CA(s) to be provided for Customer's use, Entrust will provide each Dedicated CA in accordance with the 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 the Documentation and in the Order for the Dedicated CA. The Dedicated CA and its keys will be owned and controlled by the CA. 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 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 or the Policy and Practices Documentation.

2.5. 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).

3. Grant of Rights.

3.1. 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 as part of the Certificate Services, in each case solely (a) in accordance with this Schedule and the applicable Subscriber Agreement and 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 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 (c) subject to the restrictions set out in Sections 6.2 (General Restrictions) and 6.3 (Hosted Services Restrictions) of the General Terms.

3.2. 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 3.2 (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 Schedule, the applicable Subscriber Agreement and Documentation, 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). 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 3.1 (General Use), 7 (Support Services), and 11.1 (Offering Term) 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, Responsibilities, and Representations and Warranties.

4.1. Agents. A Subscriber may exercise its rights and obligations with respect to the Certificate Services through Customer or through certain Users authorized to hold the roles as set out in Exhibit A, subject to any applicable verification or confirmation requirements set out in the Policy and Practices Documentation, 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. Customer 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.

4.2. 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.

4.3. Enterprise RA. A CA and a Subscriber may mutually agree to appoint an Enterprise RA for certain Certificates to be issued to or for Subscriber. Subscriber is responsible for ensuring that such an Enterprise

RA complies with, and maintains records showing compliance with, the requirements applicable to Enterprise RAs set out in the applicable Policy and Practices Documentation and Industry Standards. Entrust and the CA (if different) have the right to monitor the compliance of the Enterprise RA and Enterprise RA shall cooperate with such monitoring, which shall include upon request and at least annually, the provision of compliance records.

4.4. Representations and Warranties. Customer will comply with the requirements set forth in the applicable Subscriber Agreement when it acts in the capacity of Subscriber. 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 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 each Subscriber Agreement) 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 that Customer has the authority to bind all Subscribers to the Subscriber Agreement if and to the extent that such Subscribers are issued any Certificate(s) under this 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.

4.5. 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 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.

4.6. 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.

4.7. Devices. For Certificates issued to devices, Customer is responsible for ensuring that the relevant devices support and are interoperable with the Certificates. Some types of identity verification for certain Certificates require that the User use a smartphone or tablet mobile device with specified operating systems to be valid, as set out in the applicable Policy and Practices Documentation. Customer is responsible for ensuring that its Users comply with any requirements to use the specified type of device when undergoing verification.

4.8. 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.

5. Handling of Particular Information. For the purposes of this 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).

5.1. Certificate and Verification Information. Information submitted or collected as part of verification, Certificates, and information about or contained in Certificates (collectively, "Certificate and Verification Information") will be provided to all parties that may be involved in verification and issuance of Certificates, and will be processed in accordance with the Subscriber Agreement.

5.2. 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.

5.3. Cloud Content. "Cloud Content" means Certificate and Verification Information, Administration 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, any of its Affiliates, or any CA or RA 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.

5.4. 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.

5.5. 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 and each CA and RA (including any of their 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.

5.6. 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, and (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 fulfill its responsibilities under the Agreement, including demonstrating the Hosted Service or any component thereof's compliance with Industry Standards.

6. **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 Schedule).

7. **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.

8. **Interoperability**. 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. Entrust grants no rights, warranties or support for any such Interoperation Tools. 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.

9. **DISCLAIMER OF WARRANTY.** For the purposes of this 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.**

10. **INDEMNIFICATION.**

10.1. 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.

10.2. 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 5.5 (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).

11. **Offering Term and Termination.**

11.1. Offering Term. The Certificate Services are sold either on a unit basis (per Certificate license) 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 license 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.

11.2. Termination. In addition to the termination rights in the General Terms, 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.

11.3. 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) all Certificates issued under the Agreement may be revoked, and any Dedicated CAs may be de-commissioned.

12. **Suspension**. In the event that Entrust suspects any breach of the Agreement or the Policy and Practices Documentation 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. In addition, application processing and issuance of Certificates or Time-stamps may be suspended if and as required under the Policy and Practices Documentation and Industry Standards.

13. **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**.**

14. Open Source Software and Third Party Products.

14.1. 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.

14.2. Third Party Products and Services. Certain third-party hardware, software and other products 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 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:

14.2.1. 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.

14.2.2. If Customer purchases from Entrust any entitlements to any non-Entrust branded third party Certificates, such as D-Trust Certificates, such third party Certificates may be subject to the third party's own terms and conditions and may require Customer or Subscriber to authorize Entrust to act as its representative, all as detailed in specialized order forms provided at the time of purchase. Entrust shall provide support in relation to D-Trust products pursuant to the Support Schedule available at https://www.entrust.com/certificatesolutions-identity/support-schedule.pdf, and may in its discretion provide complementary Foreign Certificate Management Right(s) to facilitate management of such third party certificates.

14.3. 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.

Exhibit A

Certificate Request and Authorization

Representation of Authority

_____ ("Subscriber") agrees that it is entering or has entered into one or more legally valid and enforceable Subscriber Agreements (available at http://www.entrust.net/cps) that create extensive obligations on Subscriber in consideration for the right of Subscriber to apply for publicly-trusted digital certificates ("Certificates") to be issued by Entrust Corporation (including its affiliates, "Entrust") or by a third party certification authority contracted by Entrust (such issuer, whether Entrust or the third party, the "CA"). Public trust digital certificates serve as various forms of digital identity for Subscriber. The loss or misuse of this identity can result in great harm to the Subscriber. The individual(s) signing this Certificate Request and Authorization ("Authorization") represent(s) that they have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the Subscriber's website and other digital assets ("Authorized Subscriber Representative/Contract Signer"), and acknowledge(s) that Subscriber is responsible for all uses of its Certificates. By signing this Authorization on behalf of the Subscriber, the Authorized Subscriber Representative/Contract Signer (s) represent(s) that they i. are acting as an authorized representative of the Subscriber, ii. are expressly authorized by the Subscriber to sign Subscriber Agreements and approve Certificate requests on Subscriber's behalf, and iii. have confirmed Subscriber's rights and powers with respect to the domain(s), trademarks, code, email addresses, electronic signatures, electronic seals and other digital assets to be included in the Certificates.

Grant of Authority

The Subscriber exercises its rights and obligations with respect to Certificates issued to it through users appointed to hold administrator roles (e.g. SuperAdmin and SubAdmin) in the systems used by the CA for registration of subscribers and issuance of Certificates. Subscriber hereby expressly authorizes the individuals listed below and such other individuals assigned as administrators, Certificate Requesters or Approvers within the Entrust certificate lifecycle management tool from time to time (collectively, "Administrators") to have and exercise the permissions associated with such roles as described in the ECS console, including permission to request and approve the generation, renewal, re-issuance, and revocation of Certificates, including via APIs (each such request, a "Certificate Request") on behalf of the Subscriber.

The Subscriber hereby requests that the CA generate, renew, re-issue or revoke such Certificates, as the case may be, in accordance with each future Certificate Request submitted on behalf of the Subscriber and properly authenticated as originating with, or otherwise being approved by, its Administrator(s). The Subscriber expressly authorizes this (these) Administrator(s) to provide or authorize others to provide, the information requested from the Subscriber by the CA in connection with Certificate Requests. The Subscriber agrees that the provision of such information will be accepted as an authorized attestation of the accuracy and correctness of such information by and on behalf of the Subscriber. The Subscriber agrees that it shall be obligated under the Subscriber Agreement for all Certificates issued at the request of, or approved by, this (these) Administrator(s) until the authorization granted in this Authorization is revoked. Subscriber agrees to the methods described in the applicable CPS or service documentation for authenticating Administrators when certificate requests are approved, for periodic re-confirmation of authority for Administrators who approve certificate requests, and secure procedures for revoking authorizations and permissions granted to any Administrator.

The Subscriber has signed this Certificate Request and Authorization form through the duly appointed representative(s identified below, each of whom is meets the definition of "Authorized Subscriber Representative/Contract Signer" above.

Administrators	
Authorized Subscriber Representative/Contract Signer	

Subscriber *(as defined above), represented in this act by:*

Signature _____

Printed Name _____

Title _____

Date

And by (optional):

Signature _____

Printed Name _____

Title _____

Date _____