Entrust Certificate Services Subscription Agreement

Attention - read carefully: this Entrust Certificate Services Subscription Agreement ("**Agreement**") is a legal contract between Customer (as defined below) and Entrust (as defined below). Before continuing, please carefully read this agreement and the CPS, as amended from time to time, which is incorporated into this Agreement and which collectively contain the terms and conditions under which Customer is acquiring a limited right to use the Certificate Services.

The individual who clicks on the "accept" icon below or submits an application for Certificate Services, represents and warrants: (i) you have the legal authority to bind the Customer to the terms and conditions of this Agreement and including the CPS; (ii) Customer is legally bound by the terms of this Agreement. If you and/or the Customer do not agree to the terms and conditions of this Agreement, click on the "decline" icon below and do not continue the application process.

Please note that these terms and conditions do not apply if Entrust has entered into a separate subscription, master or other supervening agreement with the Customer relating specifically to Certificate Services.

1. **Definitions**. In addition to capitalized terms defined elsewhere in this Agreement or the CPS, the following capitalized words will have the meaning set out below:

"**Activation Date**" means the earliest of the following dates (i) the date that Entrust enables the Certificate Services for Customer's use if Customer has purchased Management Services from Entrust; (ii) the date that Customer is issued one or more Certificate(s) if Customer has not purchased Management Services from Entrust.

"**Affiliate**" means, with respect to Entrust, a person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with Entrust, and, with respect to Customer, any corporation or other entity that is directly or indirectly controlled by Customer (with "control" meaning ownership of more than fifty percent (50%) of the voting stock of the entity or, in the case of a non-corporate entity, an equivalent interest).

"**Agents**" means, in the context of (1) EV SSL Certificate(s) and EV Code Signing Certificate(s), the following individuals as defined in the CPS (i) Certificate(s) Requestor(s); (ii) Certificate(s) Approver(s); (iii) Registered Agent(s); and (iv) Contract Signer; and (2) SSL Certificate(s) and Private SSL Certificate(s), Subscriber's technical contacts as described in the CPS. In either context, Agent will also include (a) any third party who provides hosting services for Customer or Customer Affiliates ("**Web Hosters**"), or (b) any organization that digitally signs code on behalf of a Subscriber ("**Signing Authority**"). The Agents initially appointed by Customer or Customer Affiliates may be listed at Exhibit A, or will be provided to Entrust during enrollment. Such appointment may be modified using means established by Entrust from time to time.

"**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.

"**Baseline Requirements**" means; (i) the most recent version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Public Trust BRs"), and (ii) in respect to code signing Certificates, the most recent version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Code Signing BRs"). Baseline Requirements are posted on the Internet at http://www.cabforum.org/.

"**Certificate**" means a digital document that at a minimum: (a) identifies the certification authority issuing it, (b) names or otherwise identifies the Subscriber; (c) contains a public key of a key pair, (d) identifies its operational period, and (e) contains a serial number and is digitally signed by a 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) SSL Certificates, extended validation ("**EV**") SSL Certificates, code signing Certificates, EV code signing Certificates, document signing Certificates, verified mark Certificates ("**VMC**s"), mobile device Certificates, private SSL Certificates, secure email personal Certificates, secure email enterprise Certificates, eIDAS qualified website authentication Certificates ("**eIDAS QWAC**s"), PSD2 qualified website authentication Certificates ("**PSD2 QWAC**s").

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

"**Certificate Services**" means the specific services that Customer has purchased (on its own behalf and, if applicable, on behalf of the Customer Affiliates) relating to the issuance and revocation of one or more Certificate(s) under any brand that Entrust may use from time to time. Certificate Services may also include Management Services, Foreign Certificate Management Right(s) and Malware Scanning Services. Certificate Services also includes any Certificate(s) issued to Customer (and, if applicable, Customer Affiliates) by any member of the Entrust Group and licensed for use under this Agreement. Entrust reserves the right to modify the Certificate Services in its discretion during the Subscription Term.

"**Contract Signer**" means the individual who agrees to this Agreement on behalf of, and under the authority of Subscriber.

"**CPS**" means the most recent version of the certification practice statement that is incorporated by reference into this Agreement and the Certificate(s) that are issued to Subscriber, as may be amended from time to time in accordance with the terms of the CPS. 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, use of eIDAS QWACs and PSD2 QWACs is governed by the most recent version of the document titled "Certification Practice Statement For Qualified Certificates", use of private SSL Certificate(s) is governed by the most recent version of the document titled "Certification Practice Statement For Private Trust Certificates", and use of all other Certificates is governed by the most recent version of the document titled "Certification Practice Statement".

"**Customer**" means the Person who has entered into this Agreement to receive Certificate Services.

"**DPA**" means the latest version of Entrust's data processing agreement for customers, which is available at https://www.entrustdatacard.com/resource-center/licensing-and-agreements.

"**Enterprise**" means Customer and Customer Affiliates.

"**Entrust**" means Entrust, Inc. if Customer is a resident of the United States; otherwise, Entrust means Entrust Limited. "**Entrust Group**" means collectively Entrust, its Affiliates, its licensors, its Resellers, its suppliers, and the directors, officers, subcontractors, agents and personnel of any of them.

"**EV Guidelines**" means; (i) in respect to EV SSL Certificate(s), the most recent version of the CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Certificates ("EV SSL Guidelines"), and (ii) in respect to EV code signing Certificate(s), the most recent version of the CA/Browser Forum Guidelines For The Issuance And Management of Extended Validation Code Signing Certificates ("EV Code Signing Guidelines"). EV Guidelines are posted on the Internet at http://www.cabforum.org/.

"**Foreign Certificate(s)**" means any Certificate that was not issued by Customer's Management Services account under this Agreement. 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, and Certificates issued by any third party.

"**Foreign Certificate Management Right(s)**" means an optional license enabling Customer to use its Management Services account to manage (as set out in the documentation) 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 Services 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 Services account.

"**Industry Standards**" means, collectively, the most up-to-date versions of each of the following: EV Guidelines, Baseline Requirements, European Standards produced by the ETSI Technical Committee Electronic Signatures and Infrastructures, Verified Mark Guidelines, and laws and regulations, in each case, that are applicable to the various types of publicly-trusted Certificates issued by Entrust, and to which Entrust is subject and bound as an issuer of such Certificates.

"**Malware Scanning Services**" means optional daily malware scanning services that are made available with a Certificate and hosted by a third party supplier on behalf of Entrust. Each SSL Certificate includes the option to perform limited daily malware scanning for up to 250 pages and blacklist monitoring, for one domain. EV SSL Certificates include the option to perform limited daily malware scanning for up to 500 pages, blacklist monitoring, and such other ancillary scans for one domain that are documented as part of the services. Notwithstanding the foregoing, private SSL Certificates do not include Malware Scanning Services. Such Malware Scanning Services are subject to Customer supplying the information necessary to such third party supplier to perform such services and will be available until the earlier of: (i) the end of the Subscription Term; (ii) revocation of the applicable Certificate corresponding to the domain being scanned; and (iii) Malware Scanning Service discontinuation by Entrust. Entrust reserves the right to alter the features and functionality of the Malware Scanning Services or discontinue such services throughout the Subscription Term and makes no warranty that any malware, security threats or vulnerabilities will be detected or is detectable by such services.

"**Management Services**" means a self-service administration tool hosted by Entrust that is designed to help Customer manage Certificate(s) that may be made available to Customer by Entrust that enables Customer to manage the issuance, revocation, and expiry of one or more Certificate(s) issued for Customer as part of Certificate Services. Management Services are available in two (2) deployment and use models as may be described in the documentation: a certificate pooling model ("Pooling") and a non-pooling model ("Non-Pooling").

"**Permitted Group**" means (i) in the case of SSL Certificates, EV SSL Certificates, private SSL Certificates, EV code signing Certificates, document signing Certificates, code signing Certificates, and VM Certificates, Customer and Customer Affiliates; and (ii) in the case of mobile device Certificates, secure email personal Certificates and secure email enterprise Certificates ("Client Certificates"), Customer's (A) employees and (B) third parties conducting Enterprise related business to whom Enterprise has assigned an email address or mobile device for such business purposes, provided that any issuance and distribution to such third parties is done pursuant to the most recent version of the Client Certificate Agreement that can be found on the Internet at http://www.entrust.net/cps and provided that (i) Customer 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) Customer has paid the applicable license fee for the Client Certificate; and (iv) such Client Certificate is used for Enterprise related business only.

"**Person**" means and includes an individual, a legal or commercial entity (such as a corporation, business, trust, partnership, limited liability company, association, joint venture, or public corporation), and any foreign or domestic governmental authority (including any national, provincial, state, territorial, or local government authority; quasi-governmental authority; court; government organization; government commission; governmental board, bureau or instrumentality; regulatory, administrative or other agency; and any political or other subdivision, department, or branch of any of the foregoing).

"**Reseller**" means a legal entity authorized by Entrust to resell Certificate Services to Customer.

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

"**Subject**" means the Person identified in a Certificate as the holder of the private key associated with the public key given in the certificate.

"**Subscriber**" means the Person in the Permitted Group who applies for or is issued a Certificate under this Agreement.

"**Subscription Fees**" means the fees established by Entrust for use of the Certificate Services, Management Services and ECS Support Services that you have purchased, as posted from time to time at Entrust's internet web site and/or in the documentation included with the Management Services, or as set out in a quotation issued to Customer by Entrust, or as set out in a purchase order issued by Customer to Entrust (or to a Reseller) that has been accepted by Entrust. Notwithstanding the foregoing, if Customer has purchased the Certificate Services through a Reseller the Subscription Fees will be the fees agreed to between Customer and such Reseller provided that such Reseller pays to Entrust such portion of such Subscription Fees as required pursuant to the written agreement between Entrust and such Reseller.

"**Subscription Term**" means the length of time that Customer has subscribed to purchase Certificate Services commencing on the Activation Date. In the case where Customer has purchased Certificate Services that: (i) are for a single Certificate, the Subscription Term is the validity period of the applicable Certificate(s); (ii) include "Pooling" Management Services, the Subscription Term is the period of time for which Customer has purchased the right to use such Management Services, irrespective of whether the Certificate(s) that are issued to Customer as part of Certificate Services have validity periods extending beyond such period of time, or (iii) include "Non-Pooling" Management Services, the Subscription Term is the validity period of the applicable Certificate(s) issued under such Management Services, provided that all such Certificates are issued on or before the one (1) year anniversary of the Activation Date after which time such ability to request issuance shall expire. In the event that Customer elects to renew its subscription to the Certificate Services upon expiration of the Subscription Term for an additional length of time (a "Renewal Term"), the Subscription Term will be extended to include such Renewal Term upon payment of the Subscription Fees for the Renewal Term. In any case, the Subscription Term may be shortened pursuant to Section 10 (Term and Termination) of this Agreement.

"**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.

"**Valid**" means that a Certificate has not expired and has not been revoked.

"**Verified Mark Guidelines**" mean the most recent version of the guidelines approved by the Authindicators Working Group for VMCs.

2. **Operation of the PKI.** The CPS sets out Entrust's practices for managing its public-key infrastructure and providing Certificates, 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;
(g) How revocation status information is provided and the period over which it is available.

3. **Services and License.**

3.1. Issuance and Revocation of Certificate(s). Upon receipt of an application for Certificate Services, Entrust will perform limited verification (as described in the CPS) of the information submitted by Enterprise. After completing such verification, Entrust may issue Customer or Customer Affiliates (if applicable) one or more Certificate(s) (depending on the amount of Subscription Fees Customer has paid) as described in the CPS. If Entrust issues Certificate(s) services to Customer or Customer Affiliates (if applicable), Entrust will make such Certificate(s) available for retrieval. Entrust is entitled to revoke a Certificate it has issued if revocation is requested by Customer, upon expiry or termination of this Agreement, or for any other reason identified for revocation in this Agreement, the CPS or the Industry Standards.

3.2. Grant of Rights. Subject to the terms and conditions of this Agreement, Entrust hereby grants to Enterprise a non-exclusive, non-transferable right to use the Certificate Services (including, for clarity, all Certificates) solely, in the case of Certificates, for the purposes set out in the CPS, and, in the case of other Certificate Services, for the purposes set out in the applicable documentation provided with the Certificate Services. Enterprise may only deploy the number of Certificates that Enterprise has purchased from Entrust or its Reseller. Enterprise will not: (a) host, time-share, rent, lease, sell, license, sublicense, assign, distribute or otherwise transfer or allow third parties to exploit any component of the Certificate Services, except as provided in the Agreement; (b) copy, modify, translate, reverse engineer, de-compile or disassemble, or create derivative works from the Certificate Services except to the extent that law explicitly prohibits this restriction notwithstanding a contractual restriction to the contrary; (c) attempt to circumvent or disable any restriction or entitlement mechanism that is present or embedded in any component provided as part of the Certificate Services; (d) provide any passwords or other log-in information provided by Entrust as part of the Certificate Services to any third party; (e) share non-public features or content of the Certificate Services with any third party; (f) access the Certificate Services in order to build or benchmark against a competitive

product or service, or to build a product or service using similar ideas, features, or functions of the Certificate Services; (g) use the Certificate Services to send or store infringing or unlawful material or viruses, worms, time bombs, Trojan horses and other harmful or malicious codes, files, scripts, agents or programs or (h) use the Certificate Services other than in accordance with the Agreement and in compliance with all applicable Industry Standards, laws and regulations. Enterprise will not copy, modify, adapt or merge copies of the Certificate Services except as provided in this Agreement. Enterprise will not translate, reverse engineer, de-compile or disassemble the Certificate Services except to the extent that law explicitly prohibits this restriction notwithstanding a contractual restriction to the contrary.

3.3. ECS Support Services. If Customer has purchased Management Services Customer is entitled to receive the ECS Support Services set below. "**ECS Support Services**" means the maintenance, support and verification services relating to the: (i) issuance and revocation of one or more Certificate(s) to Customer or Customer Affiliates, (ii) Certificate Services, and (iii) Management Services, that are provided by Entrust according to the service plan selected and paid (if applicable) for by Customer. ECS Support Services are available in the following service plans: (i) the Silver Support Plan ("**Silver Support**"), and (ii) the Platinum Support Plan ("**Platinum Support**"). ECS Support Services are provided by Entrust for the duration of the Subscription Term pursuant to the terms and conditions of the ECS Support Services Agreement available on the Internet at www.entrust.net/cps. Entrust reserves the right to modify the ECS Support Services in its discretion during the Subscription Term. If Customer has subscribed to Management Services, Silver Support services will be provided to Customer at no additional charge as part of the Management Services that Customer has subscribed to. If Customer has subscribed to Management Services, Customer may elect to upgrade the ECS Support Services to the Platinum Support Plan, subject to Customer's payment of the applicable Subscription Fee. The Subscription Fee for the Platinum Support Plan must be paid for all Certificates in the Management Services account, or added thereafter during the Subscription Term.

3.4. Optional Software. Any computer software made available to Enterprise for download as part of the Certificate Services or as part of the ECS Support Services (including any associated support or professional services) will be licensed to Enterprise under the terms and conditions embedded in or associated with such software ("**Optional Software**"). Optional Software shall not be subject to the terms and conditions of this Agreement.

4. **Fees.** Customer will pay all applicable Subscription Fees for any Certificate Services issued to Customer. All fees are non-cancellable and non-refundable. All amounts due under this Agreement to Entrust must be paid to the Entrust Affiliate that issued the applicable invoice. Subscription Fees will be invoiced at the beginning of the Subscription Term, and Customer will pay all amounts payable within thirty (30) days of the date of the invoice, without setoff or counterclaim, and without any deduction or withholding. Customer will be responsible for any taxes (other than taxes based on Entrust's net income), fees, duties, or other similar governmental charge. Should any taxes be due, Customer will pay such taxes. Entrust may elect to charge Customer interest for late fees at the lesser of 1.5% per month or the maximum rate permitted by law. Notwithstanding any of the foregoing, if Customer has purchased through a Reseller then the terms relating to fees and taxes will be those terms established between Customer and such Reseller instead of those set out above. If payment is not received within five (5) business days of written notice that a payment is delinquent, Entrust may suspend provision of all or part of the Certificate Services, refuse to process any subsequent applications for additional Certificate Services, and revoke all Certificates.

5. **Representations, Warranties and Additional Obligations.**

5.1. Customer represents and warrants to Entrust and all Certificate Beneficiaries that Customer has the authority to bind Customer Affiliates to this Agreement (if Customer Affiliates are issued any Certificate(s) or otherwise receive any Certificate Services in connection with the Management Services purchased hereunder, if applicable).

5.2. 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.

5.3. Customer will notify all Customer Affiliates, Agents, and any other Persons who act in the capacity of Subscriber or Subject (e.g. apply for, receive, are issued, or manage Certificates) under this Agreement or through Customer's Management Services 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 such Customer Affiliates, Agents,

and Persons in connection with the Certificate Services and Certificates, and Customer will be responsible for ensuring such compliance.

6. **Confidentiality.** In this Section (Confidentiality), "Discloser" means the party that discloses Confidential Information (defined below), and "Recipient" means the party that receives it. If Confidential Information is disclosed or received by an Affiliate of a party, it is deemed to have been disclosed or received by the party itself. The Recipient will maintain in confidence all Confidential Information that it receives, and will use such Confidential Information only for the purpose of exercising its rights and fulfilling its obligations under the Agreement. Recipient will treat such Confidential Information with the same degree of care against unauthorized use or disclosure that it affords to its own information of a similar nature, but no less than reasonable degree of care. Recipient will not remove or destroy any proprietary or confidential legends or markings placed upon any documents or other materials. Recipient will only disclose Discloser's Confidential Information to Recipient's and its Affiliates' personnel and agents with a need to know ("Recipient Agents"). Recipient shall be responsible for ensuring Recipient Agents comply with the confidentiality obligations of this Section (Confidentiality) and any acts or omissions of a Recipient Agent in breach of the terms and conditions of this Section (Confidentiality) shall be considered the acts or omissions of the Recipient. "Confidential Information" means any business, technical, financial, or other information, however conveyed or presented to the Recipient, including all information derived by the Recipient from any such information that is clearly designated by the Discloser as being confidential or that ought reasonably to be considered confidential by the Recipient. Confidential Information does not include any information that: (i) is Personal Data, Verification Information or Certificate Information, which are instead subject to Section 12 (Personal Data, Verification Information and Certificate Information); (ii) was lawfully known by Recipient prior to disclosure; (iii) was lawfully in the public domain prior to its disclosure, or becomes publicly available other than through a breach of the Agreement; (iv) was disclosed to Recipient by a third party without a duty of confidentiality to the Discloser; or (v) is independently developed by Recipient without reference to Discloser's Confidential Information. If Recipient is compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law, to disclose Confidential Information of the Discloser, Recipient will use reasonable efforts to seek confidential treatment for such Confidential Information, and, if and as permitted by law, will provide prior notice to the Discloser to allow the Discloser to seek protective or other court orders. Recipient agrees that its breach of this Section (Confidentiality) may cause Discloser irreparable injury, for which monetary damages may not provide adequate compensation, and that in addition to any other remedy, Discloser may be entitled to injunctive relief against such breach or threatened breach.

7. **DISCLAIMER OF WARRANTY. Except as may be expressly stated in this Agreement (including the CPS), the Certificate Services are provided "as is", and Entrust Group disclaims any and all representations, conditions or warranties of any kind, express or implied, including warranties of non-infringement, title, merchantability or fitness for a purpose, satisfactory quality, or any representations, conditions or warranties implied by statute, course of dealing, course of performance, or usage or trade. Entrust Group makes no representations, conditions or warranties regarding any third party product or service, including any Vendor Product, or other third party product with which the Certificate Services may interoperate. Except for the express representations, warranties and conditions stated in this Agreement (including the CPS), the entire risk of the use of any Certificate Services, Certificates, and the validation of digital signatures will be borne solely by Customer.**

8. **IP INDEMNIFICATION.**

8.1. Intellectual Property Indemnity. Entrust shall defend Customer from any claims by third parties that the Certificate Services furnished and used within the scope of this Agreement infringe upon or misappropriate a Canadian, United States or European Union patent issued as of the Activation Date, trademark, copyright, trade secret or other proprietary right (a "Claim"), and will pay any damages, settlements, costs, and expenses, including without limitation court costs and reasonable attorney's fees, finally awarded against Customer by a court or arbitrator in any proceeding related to such Claim, provided, however, that Customer (i) gives to Entrust prompt written notice of each Claim threatened or received by Customer, (ii) gives to Entrust the exclusive right to control and direct the investigation, defense and settlement of such Claim, and (iii) has not compromised or settled the Claim.

8.2. Mitigation by Entrust. If (a) Entrust becomes aware of an actual or potential Claim, or (b) Customer provides Entrust with notice of an actual or potential Claim, Entrust may (or in the case of an injunction against Customer, shall), at Entrust's sole option and expense: (i) procure for Customer the right to continue to use the affected portion of the Certificate Services; (ii) modify or replace the affected portion of the Certificate Services with functionally

equivalent or superior certificate services so that Customer's use is non-infringing; or (iii) if (i) or (ii) are not commercially reasonable, revoke the affected Certificates and pay to Customer the prorated cost of the revoked Certificates, less any outstanding moneys owed on such Certificates.

8.3. Exceptions to Indemnity. Entrust shall have no liability, and shall be indemnified and held harmless by Customer against any Claim in respect of any Certificate Services if: (a) such Certificate Services are used by Customer outside the scope or the license granted in this Agreement or in a manner or for a purpose other than that for which it was supplied, as contemplated by Entrust's documentation; (b) such Certificate Services are modified by Customer without the written consent of Entrust; or (c) the Claim is based on infringement arising from: (i) the web server software that issued the certificate signing request (CSR); (ii) a certificate signing request (CSR) or any information contained therein; or (iii) information, data or specifications provided by Customer to Entrust.

8.4. **LIMIT TO INDEMNITY. THIS SECTION 8 (IP INDEMNIFICATION) IS SUBJECT TO SECTION 9 (LIABILITY) AND STATES THE SOLE AND EXCLUSIVE LIABILITY OF ENTRUST, AND THE SOLE AND EXCLUSIVE REMEDY OF SUBSCRIBER WITH RESPECT TO ANY CLAIM OF THE NATURE DESCRIBED HEREIN.**

9. **LIABILITY.**

9.1. **EXCLUSIONS. IN NO EVENT WILL ENTRUST GROUP BE LIABLE FOR, AND CUSTOMER WAIVES ANY RIGHT IT MAY HAVE TO, ANY CONSEQUENTIAL, INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE OR EXEMPLARY DAMAGES OR FOR ANY LOSS OF BUSINESS, OPPORTUNITIES, REVENUES, PROFITS, SAVINGS, GOODWILL, REPUTATION, USE, OR DATA, OR COSTS OF REPROCUREMENT OR BUSINESS INTERRUPTION, OR ANY LOSS OR DAMAGE THAT IS NOT DIRECTLY ATTRIBUTABLE TO THE USE OR RELIANCE ON A CERTIFICATE OR THE CERTIFICATE SERVICES PROVIDED UNDER THIS AGREEMENT AND THE CPS INCLUDING ANY LOSS OR DAMAGE RESULTING FROM THE COMBINATION OR INTEGRATION OF THE CERTIFICATE OR CERTIFICATE 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 OR CERTIFICATE SERVICES ALONE.**

9.2. **LIMITS. IN NO EVENT WILL ENTRUST GROUP'S TOTAL AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT, THE CPS AND THE USE AND PERFORMANCE OF ANY PRODUCTS AND SERVICES PROVIDED HEREUNDER EXCEED THE FEES PAID TO ENTRUST FOR THE APPLICABLE PRODUCT OR SERVICE FOR THE TWELVE MONTHS PRIOR TO THE EVENT GIVING RISE TO THE LIABILITY, LESS ANY REFUNDS, SERVICE CREDITS OR DEDUCTIONS.**

9.3. **APPLICATION. THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIABILITY) APPLY: (A) REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), WARRANTY, BREACH OF STATUTORY DUTY, MISREPRESENTATION, STRICT LIABILITY, STRICT PRODUCT LIABILITY, OR OTHERWISE; (B) ON AN AGGREGATE BASIS, REGARDLESS OF THE NUMBER OF CLAIMS, TRANSACTIONS, DIGITAL SIGNATURES OR CERTIFICATES; (C) EVEN IF THE POSSIBILITY OF THE DAMAGES IN QUESTION WAS KNOWN OR COMMUNICATED IN ADVANCE AND EVEN IF SUCH DAMAGES WERE FORESEEABLE; AND (D) EVEN IF THE REMEDIES FAIL OF THEIR ESSENTIAL PURPOSE. CUSTOMER ACKNOWLEDGES THAT ENTRUST HAS SET ITS PRICES AND ENTERED INTO THE AGREEMENT IN RELIANCE ON THE EXCLUSIONS AND LIMITS IN THIS SECTION (LIABILITY), WHICH FORM AN ESSENTIAL BASIS OF THE AGREEMENT.**

9.4. **Specific Exclusions. In no event will Entrust or its Affiliates 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 issued under this Agreement or the CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in this Agreement or the CPS; (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 or its Affiliates (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 but not limited to Subscribers and Relying Parties. Except to the extent expressly provided in this Agreement, in no event shall Entrust or its Affiliates 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.

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

10. **Term and Termination.** This Agreement will be in effect for the Subscription Term, however, it will terminate early if Customer or Customer Affiliates fail to comply with any of the material terms or conditions of this Agreement (including for the avoidance of any doubt, the CPS), or upon revocation by Entrust of all Certificates issued hereunder if such revocation occurs prior to the end of the Subscription Term. For clarity, breaches by Agents are deemed to be breaches by Customer. Entrust may also terminate this 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. Customer must, upon expiration of the Subscription Term or termination of the Agreement, immediately cease all use of the Certificate Services and promptly remove any Certificates issued under this Agreement from the devices and/or software in which it has been installed. Any provision of this Agreement which contemplates or requires performance after the termination of this Agreement or that must survive to fulfill its essential purpose, including the terms of this Section (Term and Termination), confidentiality, limitations and exclusions of liability, and any payment obligations, will survive the termination and continue in full force and effect until completely performed or for so long as required to fulfill its essential purpose.

11. **Security; Unauthorized Access.** Customer will take all reasonable steps to prevent unauthorized access to the Certificate Services, including by protecting passwords and other log-in information. Customer will notify Entrust immediately of any known or suspected unauthorized use of the Certificate Services or breach of its security relevant to the Certificate Services and will use commercially reasonable efforts to stop said breach. If, and to the extent that, Entrust deems it reasonably necessary to do so to respond to any actual or potential security concerns, including without limitation the security of other customers' (or their users') information or any other information or data processed by the Certificate Services, Entrust may, on written notice to the Customer, suspend provision of all or part of the applicable Certificate Services until such security concerns have been adequately addressed. Entrust must keep the Customer updated with the status of the security concerns.

12. **Personal Data, Verification Information and Certificate Information.**

12.1. Personal Data. To the extent that Entrust processes any Personal Data (as defined in the DPA) on Customer's behalf and in performance of the Agreement, the terms of the DPA, which are hereby incorporated by reference, shall apply and the parties agree to comply with such terms. Customer's acceptance of this Agreement shall be treated as acceptance and signing of the DPA (including the Standard Contractual Clauses attached to the DPA). Entrust reserves the right to update the DPA from time to time to comply with legal and regulatory requirements, and to keep current with upgrades and enhancements to its products and services. The latest version posted on Entrust's website shall always apply. Customer will ensure that Personal Data is not unnecessarily disclosed to Entrust through the application process or through its use of the Certificate Services.

12.2. Third Party Databases. In performing limited verification Entrust may determine whether the organizational identity, address, and domain name provided with an Certificate Services 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 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.

12.3. Certificate Information. Entrust may insert in a Certificate any information that is provided to Entrust in the associated application for Certificate Services, which may include Verification Information and Personal Data ("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 this Agreement and in the Entrust Privacy Policy. Customer is aware and consents that Entrust will process and/or transfer the Certificate Information in the United States and/or Canada and in any other jurisdictions where the Entrust Group maintains a presence.

12.4. Other Privacy Provisions. Except as otherwise provided in this Section (Personal Data, Verification Information and Certificate Information) or in the DPA, Entrust shall not disclose to any third party any Personal Data, Verification Information or Certificate Information that Entrust obtains in its performance of the Certificate 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 this Agreement.

13. **Use of the Entrust Secured Site-Seal.** Subject to the terms and conditions of this 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. **Third Party Products.** Customer acknowledges and agrees that certain third party vendor ("**Vendor**") products and services ("**Vendor Products**") may be made available through or in connection with the Certificate Services. Except as expressly stated in this Agreement, Entrust has no obligation and excludes all liability with respect to Vendor Products, the use of which shall be exclusively subject to the Vendor's terms, conditions and policy documents ("**Vendor Terms**") embedded in or otherwise delivered with the Vendor Products. In particular:

14.1. If Customer purchases any Sixscape Vendor Products through Entrust or in connection with the Certificate Services, use of the Sixscape Vendor 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 Datcard shall provide support in relation to the Sixscape Vendor Products pursuant to the terms and conditions of the ECS Support Services Agreement available on the Internet at www.entrust.net/cps, with the following exceptions: (a) if resolution of any incident requires changes or fixes to the Vendor Products, Entrust's sole obligation will be to escalate such incident to the Vendor; and any time periods set out in the ECS Support Services Agreement shall exclude any time during which Entrust Datcard is required to wait for a response or resolution from Vendor.

14.2. If Customer uses any WebID face-to-face verification Vendor Products, use of the WebID Vendor Products shall be subject to the WebID Vendor Terms that must be accepted prior to accessing such Vendor Products. Customer acknowledges and agrees that it will have the ability to submit Verification Information, including Personal Data, to WebID through the Management Portal, 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 Section 12 (Personal Data, Verification Information and Certificate Information) of this Agreement, and processing by WebID will be done in accordance with the WebID Vendor Terms.

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

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

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

18. **Third Party Beneficiaries**. Except for the Certificate Beneficiaries as expressly provided in the Agreement or otherwise agreed in writing by the parties, the Agreement is made solely for the benefit of the parties hereto and their respective successors and permitted assigns, and no other person or entity will have or acquire any right or benefit under the Agreement, including under the UK Contracts (Rights of Third Parties) Act 1999.

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

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

21. **Notices.** In any case where any notice or other communication is required or permitted to be given under the CPS, such notice or communication will be provided as specified in the CPS. Where any other notice or communication is required or permitted, or where the CPS does not specify a mechanism, the notice or communication will be in writing and (a) personally delivered, in which case it is deemed given and received upon receipt, or (b) sent by international air courier service with confirmation of delivery to the addresses stated below, in which case it is deemed to have been given and received when delivery is confirmed.

Notices to Customer: the address stipulated in the order.
Notices to Entrust: 1000 Innovation Drive, Ottawa, Ontario, Canada K2K 3E7

22. **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.

23. **Choice of Law.** Any disputes related to the products and services offered under the Agreement, as well as the construction, validity, interpretation, enforceability and performance of the Agreement, shall, (i) if Customer is located in the United States of America, be governed by the laws of the State of Minnesota, United States, and shall be brought in the federal and state courts located in Hennepin County, Minnesota; and (ii) if Customer is located anywhere else in the world, be governed by the laws of the Province of Ontario, Canada, and shall be brought in the provincial or federal courts sitting in Ottawa, Ontario. Each party hereby agrees that the applicable courts identified in this Section (Choice of Law) shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial, state or federal court each party waives any right that such party may have to a jury trial. To the maximum extent permitted by applicable law, the parties agree that the provisions of the United Nations Convention on Contracts for the International Sale of Goods, as amended, shall not apply to the Agreement. This Section (Choice of Law) governs all claims arising out of or related to this Agreement, including tort claims.

24. **Force Majeure.** Entrust will not be in breach of the Agreement for any delay or inability to comply with any obligation under the Agreement, and will not be responsible for any consequences thereof, to the extent that such delay or inability is caused by a Force Majeure Event, provided (i) Entrust uses reasonable efforts to limit damages to Customer and to resume complying with its obligations; and (ii) the delay or inability is not due to Entrust's failure to take reasonable measures to protect against events or circumstances of the same type as that Force Majeure Event. "Force Majeure Event" means any event or circumstance, whether or not foreseeable, that was not caused by Entrust, including acts of God or the public enemy, civil commotion/disorder, riots, insurrections, war, terrorism, malicious damage, accidents, fire, floods, hurricanes, earthquakes, storms, strikes and other labor difficulties (whether or not Entrust is in a position to concede to demands), embargoes, acts of civil or military authorities, judicial action, failure of utility, transportation or communications infrastructures (including internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges), failure or default of any superior CA, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, and acts or defaults of third party suppliers or service providers.

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

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

27. **Compliance with Applicable Laws.** Certificate Services and related information, as well as certain cryptographic techniques, software, hardware, and firmware (collectively, "Technology") that may be used in processing or in conjunction with Certificate Services may be subject to export, import, and/or use restrictions. Customer will comply in all respects with any and all applicable laws, rules and regulations and obtain all permits, licenses and authorizations or certificates that may be required in connection with Customer's and its Subscribers' and Subjects' receipt of Technology and its or their exercise of its or their rights under any part of the Agreement. Customer represents and warrants with respect to itself and each of its Affiliates, Subscribers and Subjects that: (a) it is not located in, under the control of, or a national or resident of any country to which the export of any software or technology licensed under the Agreement, or related information, would be prohibited by the applicable laws, rules or regulations of the United States, Canada or other applicable jurisdiction; (b) it is not an individual to whom the export of any software or technology licensed under the Agreement, or related information, would be prohibited by the laws of the United States, Canada or other applicable jurisdiction; and (c) it has and will comply with applicable laws, rules and regulations of the United States, Canada and other applicable jurisdiction(s) and of any state, province, or locality or applicable jurisdiction governing exports of any product or service provided by or through Entrust. Customer will not use, or permit the use of, any of the Certificate Services for any purposes prohibited by applicable laws, rules or regulations on exports, including, without limitation related to nuclear, chemical, or biological weapons proliferation.

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

29. **Language.** The definitive version of this Agreement (including the CPS) is written in English. If this Agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls.

If Customer is located in Quebec, the parties hereby confirm that they have requested that this Agreement and all related documents be drafted in English; les parties ont exigé que le présent contrat et tous les documents connexes soient rédigés en anglais.

30. **Entire Agreement.** This Agreement (including the CPS) shall constitute the entire agreement between the parties hereto in respect of the subject matter of this Agreement and all previous correspondence, understandings, proposals and other communications shall be completely superseded by the terms hereof. Any purchase order terms included or associated with any order will be of no force or effect except for the identification and quantity of the Certificate Services that are being subscribed for. Any software included in the order is distributed under the terms of the agreement that accompanies such software.

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

Exhibit A

Certificate(s) Requestor(s):
Certificate(s) Approver(s):
Contract Signer:
Web Hosters:
Technical contacts:

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:

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. Subscriber will generate (in a cryptographic module if and as required in the CPS) a new, secure, and cryptographically sound key pair to be used in association with the Certificate.
3. 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.
4. 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 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 code signing Certificates and EV code signing Certificates, in accordance with the "Data Security and Private Key Protection" provisions of the Code Signing BRs.
5. Any device storing private keys will be operated and maintained in a secure manner.
6. 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.
7. 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.
8. 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 for authorized company business in accordance with the Agreement, and will only be used on behalf of the organization listed as the Subject in such Certificates.
9. The contents of Certificates will not be improperly modified.
10. 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,
    - 10.1. 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.
    - 10.2. 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.
    - 10.3. in the case of a code signing Certificate or EV code signing Certificate, immediately, if there is evidence that the Certificate was used to sign Suspect Code.
11. Subscriber will promptly cease all use of the Certificate and the private key corresponding to the public key in such Certificate, and will remove such Certificate from the device(s) and/or software in which it was installed, upon expiration or revocation of such Certificate.

12. Subscriber will immediately respond to Entrust's instructions concerning any Key Compromise or misuse or suspected misuse of a Certificate.
13. Subscriber acknowledges and agrees that Entrust is entitled to revoke a Certificate immediately if:
    13.1. Customer breaches this Agreement.
    13.2. Entrust discovers that there has been a Key Compromise of the Certificate's private key.
    13.3. Entrust discovers that a Certificate is being used to enable criminal activities, including phishing attacks, fraud and/or the distribution of Suspect Code.
    13.4. Entrust discovers that a Certificate or the private key corresponding to the public key in the Certificate has been used to digitally sign Suspect Code.
14. 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.
15. Subscriber owns, controls, or has the exclusive right to use the domain name or email address listed in Certificate.
16. Subscriber acknowledges and agrees that Entrust is entitled to modify the Agreement when necessary to comply with any changes in Industry Standards.
17. 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.
18. In addition, in the case of Code Signing Certificates and EV Code Signing Certificates,
    18.1. 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/get-support/ssl-certificate-support/enrollment-guides/ or by contacting Entrust ("**Code Signing Best Practices**").
    18.2. 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.
    18.3. 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.
    18.4. 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.
    18.5. 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.
    18.6. 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:
        18.6.1. the Certificate is identified as a source of Suspect Code,
        18.6.2. the authority to request the Certificate cannot be verified, or
        18.6.3. the Certificate is revoked for reasons other than at Customer's request (e.g. as a result of private key compromise, discovery of malware, etc.).
    18.7. 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" a Code Signing Certificate or EV Code Signing Certificate without notice to Customer or Entrust and without regard to the revocation status of the Code Signing Certificate or EV Code Signing Certificate.
    18.8. In respect to EV code signing Certificates, Customer will only use the Certificate to sign code that complies with the requirements set forth in the EV Code Signing Guidelines.
19. In addition, in the case of eIDAS QWACs and PSD2 QWACs,
    19.1. Subscriber will comply with any requirements in the CPS for it to use a secure cryptographic device, and if so required:
        19.1.1. the Subject's private key(s) will only be used for cryptographic functions within the secure cryptographic device.
        19.1.2. if the Subject's keys are generated under control of the Subscriber or Subject, the Subject's keys will be generated within the secure cryptographic device.
    19.2. 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.

19.3. 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.
19.4. 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.
19.5. If the Subscriber or Subject generates the Subject's keys:
19.5.1. 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.
19.5.2. 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.
19.5.3. and the Subject is an individual, the Subject's private key will be maintained under the Subject's sole control.
19.5.4. and the Subject is a Person other than an individual, the Subject's private key will be maintained under the Subject's control.
19.6. 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.

20. In addition, in the case of VMCs:
20.1. Subscriber will apply for and use VMCs in accordance with and subject to the VMC Guidelines.
20.2. 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 Guidelines, 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 or PSD2 QWAC 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 secure cryptographic device, and if so required, the Subject's private key(s) will only be used for cryptographic functions with the secure 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:
5.1. and the Subject is an individual, the Subject's private key will be maintained under the Subject's sole control.
5.2. and the Subject is a Person other than an individual, the Subject's private key will be maintained under the Subject's control.
6. Subject will notify Entrust immediately:
6.1. 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.
6.2. 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.
7. 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.