Entrust Certificate Services Subscription Agreement

Attention - read carefully: this Entrust Certificate Services Subscription Agreement ("**Agreement**") is a legal contract between You (as defined below) and Entrust Datacard (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 you are 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 Subscriber to the terms and conditions of this Agreement and including the CPS; (ii) Subscriber is legally bound by the terms of this Agreement. If you do not agree to the terms and conditions of this Agreement, click on the "decline" icon below and do not continue the application process.

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 Datacard enables the Certificate Services for Your use if you have purchased Management Services from Entrust Datacard; (ii) the date that You are issued one or more Certificate(s) if you have not purchased Management Services from Entrust Datacard.

"**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) Applicant Representative(s); (iv) Confirming Person(s); (v) Legal Practitioner(s); Qualified Auditor(s); (vi) Registered Agent(s); and (vii) Contract Signer; and (2) Entrust SSL Web Server Certificate(s) and Private SSL Certificate(s), Your technical contacts as described in the CPS. In either context, Agent will also include (a) any third party who provides hosting services for You or Your Affiliates ("**Web Hosters**"), or (b) any organization that digitally signs code on behalf of a Subscriber ("**Signing Authority**"). The Agents initially appointed by You or Your Affiliates are listed as Exhibit A or as otherwise provided to Entrust Datacard during enrollment. Such listing may be modified by You using means established by Entrust Datacard from time to time.

"**Application Software Vendor**" or "**ASV**" means a developer of Internet browser software or other software that displays or uses certificates, including but not limited to KDE, Microsoft, Mozilla Corporation, Nokia Corporation, Opera Software ASA, and Red Hat, Inc.

"**Certificate(s)**" 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. In the context of this Agreement, there are various Certificate(s) Types that may be issued to You by Entrust Datacard depending upon the Certificate Services that You have purchased.

"**Certificate Beneficiaries**" means, collectively, all Application Software Vendors with whom Entrust Datacard 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 You have purchased (on behalf of Yourself and, if applicable, Your Affiliates) relating to the issuance and revocation of one or more Certificate(s) to You or Your Affiliates under any brand that Entrust Datacard 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 You (and, if applicable, Your Affiliates) by any member of the Entrust Datacard Group and licensed for use under this Agreement. Entrust Datacard reserves the right to modify the Certificate Services in its discretion during the Subscription Term.

"**Certificate(s) Types**" means the type of Certificate(s) that You are issued as part of Certificate Services. These may include extended validation (EV) multi-domain Certificate(s) ("**EV SSL Certificate(s)**"), extended validation (EV) code signing Certificate(s) ("**EV Code Signing Certificate(s)**"), Entrust SSL web server Certificate(s) ("**Standard Certificate(s)**"), advantage SSL web server Certificate(s) ("**Advantage Certificate(s)**"), unified communication multi-domain Certificate(s) ("**UCC Certificate(s)**"), wildcard Certificate(s) ("**Wildcard Certificates**"), code signing Certificate(s) ("**Code Signing Certificate(s)**"), document signing certificates ("**Document Signing**

Certificate(s)"), mobile device Certificates ("**Device Certificate(s)**"), private SSL Certificate(s) ("**Private SSL Certificate(s)**") and secure email personal certificates and secure email enterprise certificates are collectively referred to as "**Client Certificate(s)**"). Standard Certificate(s), Advantage Certificate(s), Wildcard Certificate(s) and UCC Certificate(s) are also collectively referred to as "**Entrust SSL Web Server Certificate(s)**". EV SSL Certificate(s) and EV Code Signing Certificate(s) are also collectively referred to as "**Entrust EV Certificate(s)**".

"**Client Certificate Agreement**" means the most recent version of the Client Certificate Agreement that can be found on the Internet at http://www.entrust.net/cps.

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

"**CPS**" means the most recent version of the certification practice statement that is incorporated by reference into this Agreement and the Certificate(s) that You are issued, as may be amended from time to time in accordance with the terms of the CPS. The CPS applicable to a specific Certificate(s) that You are issued in connection with Certificate Services depends on the Certificate(s) Type(s) and can be found on the Internet at http://www.entrust.net/cps or by contacting Entrust Datacard. For example, use of EV SSL Certificate(s) and EV Code Signing Certificate(s) is governed by the most recent version of the document titled "Certification Practice Statements for Extended Validation (EV) Certificates", use of Entrust SSL Web Server Certificate(s), Code Signing Certificate(s), Document Signing Certificate(s) and Client Certificates is governed by the most recent version of the document titled "Certification Practice Statement", and use of Private SSL Certificate(s) is governed by the most recent version of the document titled "Certification Practice Statement For Private Trust Certificates".

"**Enterprise**" means You, Your Agents, and Your Affiliates.

"**Entrust Datacard**" means Entrust, Inc. if You are a resident of the United States; otherwise, Entrust Datacard means Entrust Datacard Limited. "**Entrust Datacard Group**" means collectively Entrust Holdings, Inc., its subsidiaries, its licensors, its Resellers, its suppliers, and the directors, officers, employees, agents and independent contractors of any of them. "**Entrust Datacard Group Affiliates**" means collectively, Entrust Datacard Corporation and its Affiliates, where "Affiliates" means a person or entity that directly, or indirectly through one or more intermediaries, controls, is controlled by or is under common control with a party hereto (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).

"**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 Your Management Services account under this Agreement. For greater certainty, Foreign Certificate(s) may include, but is not limited to, Certificates issued from other management services accounts, Certificates purchased from Entrust Datacard's retail web site, Certificates issued from other Entrust Datacard service offerings, and Certificates issued by any third party.

"**Foreign Certificate Management Right(s)**" means an optional license enabling You to use Your Management Services account to manage (as set out in the documentation) one (1) Foreign Certificate for each Foreign Certificate Management Right(s) purchased by You. The quantity of Foreign Certificate Management Right(s) available to You will be tracked by Your Management Services account and Your 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 Your Management Services account.

"**Governmental Authority**" means any foreign or domestic 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; or any political or other subdivision, department, or branch of any of the foregoing.

"**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 Datacard. Each Entrust SSL Web Server Certificate includes the option to perform limited daily malware scanning for up to 250 pages and blacklist

monitoring, for one domain. EV SSL Certificates includes 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. For greater certainty, Private SSL Certificates do not include Malware Scanning Services. Such Malware Scanning Services are subject to You 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 Datacard. Entrust Datacard 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 Datacard that is designed to help You manage Certificate(s) that may be made available to You by Entrust Datacard that enables You to manage the issuance, revocation, and expiry of one or more Certificate(s) issued to You 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 in the case of (i) Entrust SSL Web Server Certificate(s), EV SSL Certificate(s), Private SSL Certificate(s), EV Code Signing Certificate(s), Document Signing Certificate(s) and Code Signing Certificates, You and Your Affiliates; and (ii) in the case of Client Certificates, Your employees or third parties conducting Enterprise related business with to whom You have assigned an email address for such business purposes.

"**Person**" means and includes an individual, corporation, business, trust, partnership, limited liability company, association, joint venture, Governmental Authority, public corporation, or any other legal or commercial entity.

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

"**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.

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

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

"**Subscription Term**" means the length of time that You have subscribed to purchase Certificate Services commencing on the Activation Date. In the case where You have 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 You have purchased the right to use such Management Services, irrespective of whether the Certificate(s) that are issued to You 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 You elect to renew your 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 7 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.

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

"**Your Affiliates**" means Your controlled subsidiaries who You will cause to comply with this Agreement. In this context, You control a subsidiary if You own fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control for the corporation or other entity.

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

2. **Services and License**

(a) Issuance of Certificate(s): Upon receipt of Your application for Certificate Services, Entrust Datacard will perform limited verification (as described in the CPS) of the information submitted by Enterprise. After completing such verification, Entrust Datacard may issue You or Your Affiliates (if applicable) one or more Certificate(s) (depending on the amount of Subscription Fees You have paid) as described in the CPS. If Entrust Datacard issues Certificate(s) services to You or Your Affiliates (if applicable), Entrust Datacard will make such Certificate(s) available for retrieval.

(b) Grant of License: Subject to the terms and conditions of this Agreement, Entrust Datacard hereby grants to Enterprise a non-exclusive, non-transferable license to use the Certificate Services; provided, however, that Enterprise may only use the Certificate Services (including for the avoidance of any doubt, all Certificate(s)) in compliance with this Agreement, for the sole purposes of securing communications pertaining to Enterprise related business. If the Certificate Services include Management Services, Enterprise may only use the Management Services in compliance with this Agreement for the purpose of managing Certificate(s) issued by Entrust Datacard to You or Your Affiliates. All use of the Management Services must be in accordance with the documentation supplied to You as part of the Management Services. If Entrust Datacard makes computer software available to Enterprise for download as part of the Certificate Services, such software will be licensed to Enterprise under the terms of the license agreement embedded in or associated with such software. Enterprise does not acquire any rights, express or implied, in the Certificate Services, other than those rights specified in this Agreement. Enterprise will not host, time-share, rent, lease, sell, license, sublicense, assign, distribute or otherwise transfer any component of Certificate Services, except as provided in this Agreement. If one or more enabling mechanisms ("**License String**") that provides Enterprise with access to the Certificate Services is supplied to Enterprise, Enterprise may only use such Licensing String for the purpose of using the Certificate Services and Enterprise may not copy or alter a Licensing String. Each permitted copy of all or part of any item of Certificate Services must include all copyright notices, restricted rights legends, proprietary markings and the like exactly as they appear on the copy delivered by Entrust Datacard to Enterprise. You may only deploy the number of Certificates that You have purchased from Entrust Datacard or its Reseller. 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.

(c) Lifecycle Monitoring Service: Entrust Datacard will provide You with a lifecycle monitoring service ("**LMS**"). The LMS is designed to reduce the chance of disruption of Your service which may be caused by the expiration of Your Certificate(s). Entrust Datacard will use commercially reasonable efforts to send an email to the technical contact listed in the information provided to Entrust Datacard with Your Certificate Services Application (such person referred to as "**Notice Recipient**"). Such email will inform the Notice Recipient that Your Certificate(s) is due to expire according to the user configurable parameters set out in the Management Services. In the event that the Notice Recipient changes, You can still receive a LMS email notice if You provide Entrust Datacard with updated contact information for the Notice Recipient at least sixty (60) days prior to the date that Your Certificate(s) is due to expire. You will not be eligible for the LMS if Your Notice Recipient changes and Entrust Datacard is not informed of such change within the time period set forth above.

(d) ECS Support Services: If You have purchased Management Services You are 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 You or Your Affiliates, (ii) Certificate Services, and (iii) Management Services, that are provided by Entrust Datacard according to the service plan selected and paid (if applicable) for by You. 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 Datacard 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 Datacard reserves the right to modify the ECS Support Services in its discretion during the Subscription Term.

If You have subscribed to Management Services, Silver Support services will be provided to You at no additional charge as part of the Management Services that You have subscribed to. If You have subscribed to Management Services, You may elect to upgrade the ECS Support Services to the Platinum Support Plan, subject to Your 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. **Fees**

You will pay all applicable Subscription Fees for any Certificate Services issued to You, plus any additional taxes. Such payment will be made within thirty (30) days of the receipt of an invoice from Entrust Datacard for any such Certificate Services; provided, however that if You have purchased the Certificate Services through a Reseller then the payment terms will be those terms established between You and such Reseller. In the event that You do not pay the applicable fees for any Certificate Services extended to You (or where You have purchased the Certificate Services through a Reseller and such Reseller does not pay Entrust Datacard the applicable fees for any Certificate Services in accordance with Entrust Datacard's agreement with such Reseller), Enterprise will not be entitled to use such Certificate Services (including for the avoidance of any doubt, any Certificate(s)) and Entrust Datacard may refuse to process any subsequent applications submitted by You for additional Certificate Services and revoke all Certificate(s). All amounts due under this Agreement to Entrust Datacard must be paid to the invoicing member of the Entrust Datacard Group.

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

You represent and warrant to Entrust Datacard and all Certificate Beneficiaries that You have the authority to bind Your Affiliates to this Agreement (if Your Affiliates are issued any Certificate(s) or otherwise receive any Certificate Services in connection with the Management Services purchased hereunder, if applicable). You will and You will cause Your Affiliates who receive any Certificate Services hereunder, and Your Agents, to comply with: (A) the requirements (including but not limited to providing the representations and warranties) set forth in this Agreement and, in the case of EV SSL Certificate(s) and EV Code Signing Certificate(s), the EV Guidelines, and (B) all applicable laws including, without limitation, laws relating to import, export, licensing, and data protection, as they apply to the activities contemplated under this Agreement or the right to include personal information in Certificates.

You further represent and warrant to Entrust Datacard and all Certificate Beneficiaries that:

(i) all information provided, and all representations made, by Subscriber in relation to any Certificate Services are and will be complete and accurate (and You will promptly update such information and representations from time to time as necessary to maintain such completeness and accuracy);

(ii) the Private Key corresponding to the Public Key submitted to Entrust Datacard with Your application for a Certificate(s) was created using sound cryptographic techniques and all reasonable measures have been taken to maintain sole control of, keep confidential, and properly protect the Private Key (and any associated access information or device – e.g., password or token) at all times and will operate and maintain any device storing Private Keys in a secure manner;

(iii) the Certificate(s) will not be installed or used until You have reviewed and verified the accuracy of the data in each Certificate;

(iv) in the case of Entrust SSL Certificates, EV SSL Certificates and Private SSL Certificates, the Certificate(s) will be installed only on the server(s) that are accessible at the domain name (subjectAltName(s)) listed on the Certificate;

(v) Certificates and the Private Key corresponding to the Public Key listed in such Certificate will only be used in compliance with all applicable laws, solely for authorized company business, solely in accordance with the Agreement and the Certificate will not be used for any hazardous or unlawful (including tortious) activities;

(vi) You will immediately respond to Entrust Datacard's instructions concerning (1) compromise of the Private Key associated with any Certificate, and (2) misuse or suspected misuse of a Certificate;

(vii) all use of the Certificate and its associated Private Key will cease immediately, and You will promptly notify Entrust Datacard and request the revocation of the Certificate, if (1) any information included in Your application for a Certificate or the Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Certificate incorrect, misleading or inaccurate; or (2) there is any actual or suspected misuse or compromise of the Private Key (or key activation data) associated with the Public Key in the Certificate;

(viii) all use of the (1) Certificate and (2) Private Key associated with the Public Key in such Certificate will cease upon expiration or revocation of such Certificate, and such Certificate will be removed from the device(s) and/or software in which it has been installed;

(ix) You acknowledge and agree that Entrust Datacard is entitled to revoke a Certificate immediately if: (1) You breach any of Your obligations, representations and/or warranties set out in this Section 4, (2) Entrust Datacard discovers that the Private Key has been compromised, or (3) Entrust Datacard discovers that a Certificate is being used to enable phishing attacks, fraud and/or the distribution of Suspect Code;

(x) the subject named in the Certificate(s) corresponds to the Subscriber, and that the Subscriber has authorized the inclusion of such information in the Certificate;

(xi) You have the exclusive right to use the domain name or email address listed in Certificate;

(xii) in the case of Code Signing Certificates and EV Code Signing Certificates, (1) You 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 Datacard; (2) You will not knowingly use the Certificate and the Private Key corresponding to the Public Key listed in such Certificate to digitally sign Suspect Code and You acknowledge that Entrust Datacard will revoke such Certificate if You fail to comply; (3) in the event that there is evidence that a Certificate was used to digitally sign Suspect Code; (A) all use of such Certificate and its associated Private Key will cease immediately, and (B) You will immediately notify Entrust Datacard and request the revocation of the applicable Certificate if You become aware (by whatever means) that the Private Key associated with such Certificate has digitally signed code that contains Suspect Code; (4) You will not request a Certificate containing a Public Key that is, or will be used with any other Certificate Type; (5) You acknowledge and agree (A) if the Certificate is identified as a source of Suspect Code, (B) the authority to request the Certificate cannot be verified, or (C) the Certificate is revoked for reasons other than at Your request (e.g. as a result of private key compromise, discovery of malware, etc.), then Entrust Datacard is authorized to share information about the Certificate, signed application, Certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum; and (6) You acknowledge that ASV's may independently determine that a Certificate is malicious or compromised and that ASV's 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 You or Entrust Datacard and without regard to the revocation status of the Code Signing Certificate or EV Code Signing Certificate; and

(xiii) in respect to EV Code Signing Certificates; You will only digitally sign code that complies with the requirements set forth in the EV Code Signing Guidelines.

You expressly agree that You will:

a) provide, in any communications with Entrust Datacard, correct information with no known errors, misrepresentations, or omissions;
b) generate a new, secure, and cryptographically sound Key Pair to be used in association with the Certificate;
c) ensure that any information provided to Entrust Datacard in connection with Your application for a Certificate 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;
d) refrain from modifying the contents of Certificates;
e) use Certificates and Certificate Services exclusively for legal and authorized purposes in accordance with the terms and conditions of the Agreement and applicable laws;
f) only use Certificates on behalf of the organization listed as the Subject in such Certificates;
g) keep confidential and properly protect the Private Keys;
h) notify Entrust Datacard as soon as reasonably practicable of any change to any information included in Your application for a Certificate or any change in any circumstances that would make the information in Your application for a Certificate misleading or inaccurate;

i) notify Entrust Datacard as soon as reasonably practicable of any change to any information included in the Certificate or any change in any circumstances that would make the information in the Certificate misleading or inaccurate;
j) immediately cease to use Certificates if any information included in the Certificate or if any change in any circumstances would make the information in the Certificate misleading or inaccurate;
k) notify Entrust Datacard immediately of any suspected or actual Compromise of the Private Keys and request the revocation of such Certificate;
l) immediately cease to use the Certificate upon (a) expiration or revocation of such Certificate, or (b) any suspected or actual Compromise of the Private Key corresponding to the Public Key in such Certificate, and remove such Certificate from the devices and/or software in which it has been installed;
m) will comply with all applicable laws including, without limitation, laws relating to import, export, licensing, and data protection, as they apply to the activities contemplated under this Agreement including without limitation Enterprise's right to export, import or use the Certificate Services or the right to include personal information in Certificates;
n) in respect to Document Signing Certificates, generate and protect the Key Pair in a cryptographic module that (a) prevents exportation or duplication, and (ii) meets or exceeds FIPS 140-2 Level 2 certification standards;
o) refrain from using the Private Key corresponding to the Public Key in the Certificate to sign other Certificate(s); and
p) use appropriate judgment about whether it is appropriate, given the level of security and trust provided by Certificate, to use Certificate in any given circumstance.

For the avoidance of any doubt, (1) Entrust Datacard will not be under any obligation to issue any Certificate containing pre-qualified information if such pre-qualified information is subsequently found to have changed or to be in any way inaccurate, incorrect, or misleading; (2) by submitting a request for Certificate, You are representing and warranting that the pre-qualified information has not changed and is in no way inaccurate, incorrect, or misleading; (3) Entrust Datacard shall be entitled to revoke a Certificate issued to You if (i) the pre-qualified information submitted by You is subsequently found to have changed or to be inaccurate, incorrect, or misleading, (ii) if revocation is requested by You, (iii) upon expiry or termination of this Agreement, or (iv) for any other reason identified for revocation in the CPS or the applicable EV Guidelines; (4) You must notify Entrust Datacard immediately of any change to any information included in any Certificate issued to You or any Certificate management service application submitted by You or any change circumstances that would make the information in any such Certificate or Certificate Management Service application inaccurate, incorrect, or misleading, and (5) You must notify Entrust Datacard immediately of any changes to pre-qualified information, or any changes in any circumstances that would make any pre-qualified information inaccurate, incorrect, or misleading.

Client Certificates and Mobile Device Certificates may be issued and distributed to third parties within the Permitted Group, provided that such issuance and distribution is done pursuant to the Client Certificate Agreement and provided that (i) You have 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) You have paid the applicable license fee for the Client Certificate; and (iv) such Client Certificate is used for Enterprise related business only.

5. **Confidentiality**

You acknowledge that the Certificate Services (and any information incorporated therein or provided thereto) contain the confidential information of Entrust Datacard. You will not translate, reverse engineer, de-compile, disassemble, or develop competitive Certificate Services using any such information derived from Entrust Datacard's confidential information. You will retain Entrust Datacard's confidential information in confidence and will use, disclose, and copy it solely for the purpose of, and in accordance with the Agreement. You will only disclose Entrust Datacard's confidential information to Your employees and Enterprise employees with a need to know. You will use the same degree of care as You use to protect Your own confidential information of a similar nature, but no less than reasonable care, to prevent the unauthorized use or disclosure of Entrust Datacard's confidential information.

You will not be bound by any obligations restricting disclosure and use set forth in this Agreement with respect to Entrust Datacard's confidential information, or any part thereof, which: (i) was known to You prior to disclosure, without any obligation of confidentiality; (ii) was lawfully in the public domain prior to its disclosure, or becomes publicly available other than through a breach of this Agreement; (iii) was disclosed to You by a third party, provided

that such third party is not in breach of any confidentiality obligation in respect of such information; or (iv) is independently developed by You.

If You are compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law, to disclose the confidential information of Entrust Datacard, You will use reasonable efforts to seek confidential treatment for such confidential information, and provide prior notice to Entrust Datacard to allow Entrust Datacard to seek protective or other court orders.

6. **Intellectual Property Ownership**

The Certificate Services and all modifications, enhancements and derivative works thereof, including all right, title and interest (and all intellectual proprietary rights therein) remain the sole and exclusive property of Entrust Datacard and/or its third-party licensors.

7. **DISCLAIMER OF WARRANTY**

EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES, AND CONDITIONS PROVIDED IN THIS AGREEMENT AND THE CPS, CERTIFICATE SERVICES AND ANY SERVICES PROVIDED IN RESPECT TO CERTIFICATE(S) ARE PROVIDED "AS IS", AND NEITHER ENTRUST DATACARD GROUP, ENTRUST DATACARD GROUP AFFILIATES NOR ANY RESELLERS, CO-MARKETERS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING MAKE ANY REPRESENTATIONS OR GIVE ANY WARRANTIES, OR CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST DATACARD GROUP, ENTRUST DATACARD GROUP AFFILIATES, AND ALL RESELLERS, CO-MARKETERS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING SPECIFICALLY DISCLAIM ANY AND ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SATISFACTORY QUALITY, OR FITNESS FOR A PARTICULAR PURPOSE. EXCEPT FOR THE EXPLICIT REPRESENTATIONS, WARRANTIES AND CONDITIONS CONTAINED IN THIS AGREEMENT AND IN THE CPS, THE ENTIRE RISK OF THE USE OF ANY CERTIFICATE SERVICES OR ANY SERVICES PROVIDED IN RESPECT CERTIFICATE SERVICES OR THE VALIDATION OF DIGITAL SIGNATURES WILL BE BORNE SOLELY BY YOU.

8. **LIMITATION OF LIABILITY**

8.1 ENTRUST DATACARD, ENTRUST DATACARD GROUP AND ENTRUST DATACARD GROUP AFFILIATES AND ANY RESELLERS, CO-MARKETERS, SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, AND EMPLOYEES AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, "ENTRUST DATACARD AND ITS ENTITIES") SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR IN ANY OTHER WAY (EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR:

- **(I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS);**
- **(II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE;**
- **(III) ANY LOSS OF GOODWILL OR REPUTATION;**
- **(IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES, OR**
- **(V) 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, WITHOUT LIMITATION, 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 DATACARD IF THE LOSS OR DAMAGE WOULD NOT HAVE OCCURRED AS A RESULT OF USE OF THE CERTIFICATE OR CERTIFICATE SERVICES ALONE.**

IN ANY CASE WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION OF, USE OF OR RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR CERTIFICATE SERVICES (INCLUDING, WITHOUT LIMITATION, ANY ECS SUPPORT SERVICES) UNDER THIS AGREEMENT, THE APPLICABLE CPS OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

8.2 IN NO EVENT SHALL THE TOTAL AGGREGATE LIABILITY OF ENTRUST DATACARD AND ITS ENTITIES TO ANY APPLICANT, SUBSCRIBER, RELYING PARTY OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION ARISING OUT OF OR RELATING TO THIS AGREEMENT, THE CPS AND ALL CERTIFICATES ISSUED (INCLUDING WITHOUT LIMITATION, THE INSTALLATION OF, USE OF OR RELIANCE UPON A CERTIFICATE) AND THE CERTIFICATE SERVICES PROVIDED UNDER THIS AGREEMENT UNDER ANY CAUSE OF ACTION, OR ANY CONTRACT, STRICT LIABILITY, TORT (INCLUDING NEGLIGENCE), OR OTHER LEGAL OR EQUITABLE THEORY OR IN ANY OTHER WAY, EXCEED THE GREATER OF ONE THOUSAND UNITED STATES DOLLARS ($1,000.00 U.S.), OR (2) TWO TIMES THE FEES PAID BY YOU TO ENTRUST DATACARD UNDER THIS AGREEMENT DURING THE TWELVE MONTHS PRIOR TO THE INITIATION OF THE CLAIM TO A MAXIMUM OF ONE HUNDRED THOUSAND DOLLARS ($100,000.00) (EXCEPT THAT FOR ANY ENTRUST EV CERTIFICATES ISSUED UNDER THIS AGREEMENT, ENTRUST DATACARD AND ITS ENTITIES' AGGREGATE LIABILITY IS LIMITED TO TWO THOUSAND U.S. DOLLARS (US$2,000.00) PER SUBSCRIBER OR RELYING PARTY PER EV CERTIFICATE, UP TO A MAXIMUM OF ONE HUNDRED THOUSAND U.S. DOLLARS (US$100,000.00)).

8.3 THE FOREGOING LIMITATIONS WILL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN AND EVEN IF ENTRUST DATACARD AND ITS ENTITIES HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES. BECAUSE SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO YOU AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULL EXTENT PERMITTED BY LAW. THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION. THE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND THE LIMITATIONS OF LIABILITY IN THIS AGREEMENT CONSTITUTE AN ESSENTIAL PART OF THIS AGREEMENT. ALL SUBSCRIBERS, RELYING PARTIES, AND OTHER PERSONS, ENTITIES, AND ORGANIZATIONS ACKNOWLEDGE THAT BUT FOR THESE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND LIMITATIONS OF LIABILITY, ENTRUST DATACARD WOULD NOT ISSUE CERTIFICATE(S) TO SUBSCRIBERS OR PROVIDE THE CERTIFICATE SERVICES AND THAT THESE PROVISIONS PROVIDE FOR A REASONABLE ALLOCATION OF RISK.

8.4 In no event will Entrust Datacard or Entrust Datacard Group Affiliates be liable for any damages to Applicants, Subscribers, Relying Parties or any other person, entity or organization 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 Datacard or Entrust Datacard Group 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. In no event shall Entrust Datacard or Entrust Datacard Group Affiliates be liable to the Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

9. **Term**

This Agreement will continue for the Subscription Term, however, it will terminate if You, Your Affiliates, or Your Agents fail to comply with any of the material terms or conditions of this Agreement (including for the avoidance of any doubt, the CPS and in the case of EV SSL Certificates and EV Code Signing Certificate(s), the EV Guidelines). Enterprise will immediately cease to use the Certificate Services upon the earlier of (a) expiration of the Subscription Term; or (b) upon a breach of this Agreement (including the CPS) by either You, Your Affiliates or Your Agents. Entrust Datacard may also terminate this Agreement in its discretion with notice to You in order to comply with any third party licensing or other contractual or legal obligation to which Entrust Datacard is subject. This Agreement will terminate upon expiration of the Subscription Term or revocation by Entrust Datacard of all Certificates issued hereunder if such revocation occurs prior to the end of the Subscription Term. You must, upon such expiration cease all use of Your Certificate Services and remove any Certificates issued under this Agreement from the devices and/or software in which it has been installed. The provisions entitled "Representations, Warranties And Additional Obligations", "Confidentiality", "Intellectual Property Ownership", "Disclaimer of Warranties", "Limitation of Liability",

"Term", "Severability", "Audit Right", "Third Party Beneficiaries", "Entire Agreement", and those provisions of the CPS that are designated as surviving termination will continue in force even after any termination or expiration of this Agreement. All payment obligations will survive termination.

10. **Severability**

Whenever possible, each provision of this Agreement, the CPS, any other agreements will be interpreted in such manner as to be effective and valid under applicable law. If the application of any provision of this Agreement, the CPS, any other agreements or any portion thereof to any particular facts or circumstances will be held to be invalid or unenforceable by an arbitrator or court of competent jurisdiction, then (i) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of this Agreement, the CPS, or any other agreements will not in any way be affected or impaired thereby, and (ii) such provision will be enforced to the maximum extent possible so as to effect its intent and it will be reformed without further action to the extent necessary to make such provision valid and enforceable.

FOR GREATER CERTAINTY, IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EVERY PROVISION OF THIS AGREEMENT, THE CPS, AND ANY OTHER AGREEMENTS THAT DEALS WITH (I) LIMITATION OF LIABILITY OR DAMAGES, (II) DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, CONDITIONS, OR LIABILITIES, OR (III) INDEMNIFICATION, IS EXPRESSLY INTENDED TO BE SEVERABLE FROM ANY OTHER PROVISIONS OF THIS AGREEMENT, THE CPS, AND ANY OTHER AGREEMENTS AND WILL BE SO INTERPRETED AND ENFORCED.

11. **Third Party Databases**

In performing limited verification Entrust Datacard may determine whether the organizational identity, address, and domain name provided with Your Certificate Services Application are consistent with information contained in third-party databases (the "Databases"). Entrust Datacard may perform an investigation which may attempt to confirm Your business name, street address, mailing address, telephone number, line of business, year started, number of employees, CEO, telephone number and Your business existence. You acknowledge that some of the information submitted to obtain Certificate Services may become included in the Databases. This information will only include: business name, street address, mailing address, telephone number (outside source), line of business, year started, number of employees, CEO, telephone number and Your business existence.

12. **Use of the Entrust Secured Site-Seal**

Subject to the terms and conditions of this Agreement, You may use Your Certificate Services with the Entrust Secured Site-Seal; provided, however that (i) Entrust Datacard delivers to You the Entrust Secured Site-Seal together with, or in conjunction with, Your Certificate Services; and (ii) **BY CLICKING THE "ACCEPT" ICON BELOW AND BY USING THE ENTRUST SECURED SITE-SEAL, YOU AGREE TO BE BOUND BY THE TERMS AND CONDITIONS OF THE ENTRUST SECURED SITE-SEAL LICENSE AGREEMENT SET FORTH AT** http://www.entrust.net/cps**.**

13. **Export**

Certificate Services and related information may be subject to export, import, and/or use restrictions. You will comply with all laws and regulations applicable to Your right to export, import, and/or use Certificate Services or related information, including, without limitation, all laws and regulations in respect to nuclear, chemical or biological weapons proliferation. You will be responsible for procuring all required licenses and permissions for any export, import, and/or use of Certificate Services or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with Certificate Services may be subject to export, import, and/or use restrictions. You will comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use such Technology or related information. You will be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

14. **Third Party Beneficiaries**

You expressly acknowledge that each Application Software Vendor and each member of the Entrust Datacard Group and Entrust Datacard Group Affiliates are express third party beneficiaries, and may enforce this Agreement against Enterprise and rely on all terms of this Agreement.

15. **Governing Law**

The laws of the Province of Ontario, Canada, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of the Agreement. The application of the United Nations Convention on Contracts for the International Sale of Goods to the Agreement is expressly excluded. Any dispute arising out of or in respect to the Agreement shall be brought in the provincial or federal courts sitting in Ottawa, Ontario, and each party hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial or federal court each party waives any right that such party may have to a jury trial.

16. **Language**

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.

17. **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.

Exhibit A

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