ENTRUST CERTIFICATE SERVICES

Certification Practice Statement

Version: 2.16
February 1, 2017

Revision History

Issue	Date	Changes in this Revision
1.0	May 26, 1999	Initial version.
2.0	July 1, 2000	Addition of provisions dealing with subordinate entities (such as third party registration authorities) in the Entrust.net SSL Web Server public key infrastructure. Revision of numerous other terms and conditions.
2.01	May 30, 2001	Minor revisions having no substantive impact.
2.02	January 1, 2002	Minor revisions related to replacement Cross Certificate.
2.03	January 1, 2003	Entrust legal name change.
2.04	August 20, 2003	Minor revisions related to use of certificates on more than one server; permitting use of asterisk in Subject name
2.05	November 28, 2003	Minor revisions to language to handle licensing issues.
2.06	May 14, 2004	Minor revisions to language for export requirements.
2.1	August 1, 2007	Minor revisions to ensure consistency with the CPS for EV SSL Certificates and to add OCSP references.
2.2	August 11, 2008	Minor revisions to terminology to replace references to Entrust SSL Web Server Certificates with Entrust SSL Certificates. Revision to authentication of individuals, routine rekey and key changeover. Other minor revisions having no substantive impact.
2.3	September 8, 2009	Updates for Code Signing and Client Certificates. Added Appendix A with Certificate Profiles. Revisions to add additional application software vendors and relying parties as third party beneficiaries. Deleted Subscriber notice requirements.
2.4	August 16, 2010	Updates for Class 1 and 2 Client Certificates and Document Signing Certificates
2.5	December 1, 2010	Updates for Time-Stamp Certificates and end entity certificate key sizes
2.6	February 28, 2011	Update disaster recovery, time-stamp authority and code signing certificate requirements
2.7	March 1, 2012	Update to restrict use of certificates for MITM transactions or “traffic management”; Update to enable Entrust to request additional info from customers

2.8	June 25, 2012	Update for compliance to Baseline Requirements
2.9	May 1, 2013	Update for inclusion of data controls for certificate renewal, private key control, and subordinate CA certificates
2.10	December 1, 2013	Support for smartcards and subordinate CA assessment
2.11	March 4, 2014	Change to Loss Limitations
2.12	April 6, 2015	Updated PKI hierarchy, SSL SHA-2 and added Certification Authority Authorization
2.13	February 12, 2016	Update for Document Signing, Security Module and Subscriber obligations
2.14	March 7, 2016	Remove references to 1024-bit root and update approved key sizes
2.15	September 19, 2016	CT logging for SSL certificates, ECC key usage update and Document Signing key usage update
2.16	February 1, 2017	Update for Minimum Requirements for Code Signing, minimum key size and validity period, changes to Definitions, Disclaimers, Loss Limitations and Conflict of Provisions

TABLE OF CONTENTS

1. Introduction

Entrust Limited ("Entrust") uses Entrust's award winning Entrust Authority™ family of software products to provide standards-compliant digital certificates that enable more secure on-line communications.

The Entrust Certificate Services Certification Authorities issue Entrust Certificates, as defined in §10, which include the following Certificate Types:

- SSL Certificate(s) ("Entrust SSL Certificate(s)" and "Entrust SSL Web Server Certificate(s)")
- Code Signing Certificate(s) ("Entrust Code Signing Certificate(s)")
- Client Certificate(s) ("Entrust Client Certificate(s)")
- Document Signing Certificate(s) ("Entrust Document Signing Certificate(s)")
- Time-Stamp Certificates(s) ("Entrust Time-Stamp Certificates(s)")

1.1 Overview

This Entrust CPS describes the practices and procedures of (i) the Entrust Certification Authorities, and (ii) Registration Authorities operating under the Entrust Certification Authorities. This Entrust CPS also describes the terms and conditions under which Entrust makes Certification Authority and Registration Authority services available in respect to Entrust Certificates. This Entrust CPS is applicable to all persons, entities, and organizations, including, without limitation, all Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and any other persons, entities, or organizations that have a relationship with (i) Entrust in respect to Entrust Certificates and/or any services provided by Entrust in respect to Entrust Certificates, or (ii) any Registration Authorities operating under an Entrust Certification Authorities, or any Resellers or Co-marketers providing any services in respect to Entrust Certificates. This Entrust CPS is incorporated by reference into all Entrust Certificates issued by Entrust Certification Authorities. This Entrust CPS provides Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and other persons, entities, and organizations with a statement of the practices and policies of the Entrust Certification Authorities and also of the Registration Authorities operating under the Entrust Certification Authorities. This Entrust CPS also provides a statement of the rights and obligations of Entrust, any third parties that are operating Registration Authorities under the Entrust Certification Authorities, Applicants, Subscribers, Relying Parties, Resellers, Co-marketers and any other persons, entities, or organizations that may use or rely on Entrust Certificates or have a relationship with an Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority in respect to Entrust Certificates and/or any services in respect to Entrust Certificates.

Entrust conforms to the current version of the CA/Browser Forum Guidelines Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") published at http://www.cabforum.org. The Baseline Requirements describe certain minimum requirements that a Certification Authority (CA) must meet in order to issue SSL Certificates. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this CPS.

Entrust conforms to the current version of the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Minimum Requirements for Code Signing") published at https://aka.ms/csbr. The Minimum Requirements for Code Signing describe the minimum requirements for Code Signing Certificates. If there is any inconsistency between this document and the Minimum Requirements for Code Signing, the Minimum Requirements for Code Signing take precedence over this document.

1.2 Identification

This document is called the Entrust Certificate Services Certification Practice Statement.

1.2.1 End Entity Entrust Certificates

Each Certificate issued by the Entrust CA to a Subscriber contains an Object Identifier (OID) in the certificate's certificatePolicies extension that:

1. indicates which Entrust CA policy statement (i.e. this CPS) relates to that certificate, and which
2. asserts the Entrust CA's adherence to and compliance with this CPS.

The following OIDs have been registered for inclusion in Entrust Certificates:

Entrust SSL Certificates:	**2.16.840.1.114028.10.1.5** **2.23.140.1.2.2**
Entrust Code Signing Certificates:	**2.16.840.1.114028.10.1.3** **2.23.140.1.4.1**
Entrust Client Certificates:	
Class 1:	**2.16.840.1.114028.10.1.4.1**
Class 2:	**2.16.840.1.114028.10.1.4.2**
Entrust Document Signing Certificates:	**2.16.840.1.114028.10.1.6**
Entrust Time-Stamp Certificates:	**2.16.840.1.114028.10.1.7**

Entrust Certificates issued with the OID 2.23.140.1.2.2 are issued and managed in accordance with the requirements of the Baseline Requirements. Entrust Certificates issued with the OID 2.23.140.1.4.1 are issued and managed in accordance with the requirements of the Minimum Requirements for Code Signing.

1.2.2 Subordinate CA Certificates

Each Certificate issue by the Entrust CA to a Subordinate CA contains a certificate policy OID. Details about Subordinate CA Certificates specified in Appendix B.

Subordinate CA Certificates issued to an Entrust CA will contain either the policy OID or an OID identifying the specific policy for that CA.

Subordinate Certificates issued to a third party CA will contain a policy OID identifying the specific policy for that CA.

1.3 Community and Application

1.3.1 Certification Authorities

In the Entrust public-key infrastructure, Certification Authorities may accept Certificate Signing Requests (CSRs) and Public Keys from Applicants whose identity has been verified as provided herein by an Entrust-operated Registration Authority or by an independent third-party Registration Authority operating under an Entrust Certification Authority. If an Entrust Certificate Application is verified, the verifying Registration Authority will send a request to an Entrust Certification Authority for the issuance of an Entrust Certificate. The Entrust Certification Authority will create an Entrust Certificate containing the Public Key and identification information contained in the request sent by the Registration Authority to that Entrust Certification Authority. The Entrust Certificate created in response to the request will be digitally signed by the Entrust Certification Authority.

Only Certification Authorities authorized by Entrust are permitted to issue Entrust Certificates. In the event that more than one Certification Authority is authorized to issue Entrust Certificates, Entrust will post a list of authorized Certification Authorities in the Entrust Repository.

1.3.2 Registration Authorities

In the Entrust public-key infrastructure, Registration Authorities under the Entrust Certification Authorities may accept Entrust Certificate Applications from Applicants and perform a limited verification of the information contained in such Entrust Certificate Applications. The information provided is verified according to the procedures established by the Entrust Policy Authority. A Registration Authority operating under an Entrust Certification Authority may send a request to such Entrust Certification Authority to issue an Entrust Certificate to the Applicant.

Only Registration Authorities authorized by Entrust are permitted to submit requests to an Entrust Certification Authority for the issuance of Entrust Certificates.

1.3.3 End Entities

End entities for the Entrust public-key infrastructure consist of:

1. **Applicants** - An Applicant is a person, entity, or organization that has applied for, but has not yet been issued an Entrust Certificate.
2. **Subscribers** - A Subscriber is a person, entity, or organization that has been issued an Entrust Certificate.
3. **Relying Parties** – A Relying Party is a person, entity, or organization that relies on or uses an Entrust Certificate and/or any other information provided in an Entrust Repository to verify the identity and Public Key of a Subscriber and/or use such Public Key to send or receive encrypted communications to or from a Subscriber.

Additionally, Certificate Beneficiaries are express third party beneficiaries of this CPS and all agreements into which it is incorporated.

1.3.4 Applicability

This Entrust CPS is applicable to the following Certificate Types issued by Entrust Certification Authorities.

Entrust SSL Certificates

SSL Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols. Entrust SSL Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of an SSL Certificate is to facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a secure server.

Entrust Code Signing Certificates

Code Signing Certificates are used by content and software developers and publishers to digitally sign executables and other content. Entrust Code Signing Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of a Code Signing Certificate is to provide a method of ensuring that an executable object has come from an identifiable software publisher and has not been altered since signing.

Entrust Client Certificates

Client Certificates are used by individuals to digitally sign and encrypt electronic messages via an S/MIME compliant application. Entrust Client Certificates conform to the requirements of the ITU-T X.509 v3 standard. The primary purpose of a Client Certificate is to provide authentication, message integrity and non-repudiation of origin (using digital signatures) and privacy (using encryption).

Entrust Document Signing Certificates

Document Signing Certificates are used by individuals to digitally sign and encrypt electronic documents. Entrust Document Signing Certificates conform to the requirements of the ITU-T X.509 v3 standard. Document Signing Certificates help to provide authentication and document integrity.

Entrust Time-Stamp Certificates

Time-Stamp Certificates are used by individuals to digitally sign time-stamp responses. Entrust Time-Stamp Certificates conform to the requirements of the ITU-T X.509 v3 standard. Time-Stamp Certificates help to provide authentication and time-stamp token integrity.

1.4 Certificate Usage

1.4.1 Certificate Issued to Individuals

Entrust Certificates issued to individuals are typically used to sign and encrypt e-mail and to authenticate to applications (client authentication).

1.4.2 Certificates Issued to Organizations

Entrust Certificates issued to organizations are typically used for server authentication, SSL/TLS secure sessions, and code signing.

1.4.3 Assurance Levels

Class 1 Certificates is considered to be low assurance, as the verification method simply confirms that the Subscriber controls the asserted email address. No verification checks of the Subscriber's identity are performed.

Class 2 Certificates provide a greater level of assurance over Class 1 Certificates, because in addition to email address control, basic verification steps are performed to confirm the identity of the Subscriber.

1.5 Contact Details

1.5.1 Specification Administration Organization

The Entrust CPS is administered by the Entrust Policy Authority; it is based on the policies established by Entrust Limited.

1.5.2 Contact Person

The contact information for questions about Entrust Certificates is:

Entrust Limited
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
Attn: Entrust Certificate Services

Tel: 1-866-267-9297 or 1-613-270-2680
Email: ecs.support@entrustdatacard.com

2. General Provisions

2.1 Obligations

2.1.1 Certification Authority Obligations

An Entrust Certification Authority shall:

(i) provide Certification Authority services in accordance with the terms and conditions of the Entrust CPS;
(ii) upon receipt of a request from a Registration Authority operating under such Entrust Authority, issue an Entrust Certificate in accordance with the terms and conditions of the Entrust CPS;
(iii) make available Entrust Certificate revocation information by issuing Entrust Certificates and by issuing and making available Entrust Certificate CRLs in an Entrust Repository in accordance with the terms and conditions of the Entrust CPS;
(iv) issue and publish Entrust Certificate CRLs on a regular schedule in accordance with the terms and conditions of the Entrust CPS; and
(v) upon receipt of a revocation request from a Registration Authority operating under such Entrust Certification Authority, revoke the specified Entrust Certificate in accordance with the terms and conditions of the Entrust CPS.

In operating the Entrust Certification Authorities, Entrust may use one or more representatives or agents to perform its obligations under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements, provided that Entrust shall remain responsible for its performance.

2.1.2 Registration Authority Obligations

A Registration Authority operating under an Entrust Certification Authority shall:

(i) receive Entrust Certificate Applications in accordance with the terms and conditions of the Entrust CPS;
(ii) perform, log and secure limited verification of information submitted by Applicants when applying for Entrust Certificates, and if such verification is successful, submit a request to an Entrust Certification Authority for the issuance of an Entrust Certificate, all in accordance with the terms and conditions of the Entrust CPS;
(iii) receive and verify requests from Subscribers for the revocation of Entrust Certificates, and if the verification of a revocation request is successful, submit a request to an Entrust Certification Authority for the revocation of such Entrust Certificate, all in accordance with the terms and conditions of the Entrust CPS;
(iv) notify Subscribers, in accordance with the terms and conditions of the Entrust CPS, that an Entrust Certificate has been issued to them; and
(v) notify Subscribers, in accordance with the terms and conditions of the Entrust CPS that an Entrust Certificate issued to them has been revoked or will soon expire.

Entrust may use one or more representatives or agents to perform its obligations in respect of an Entrust-operated Registration Authority under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements, provided that Entrust shall remain responsible for the performance of such representatives or agents under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust may appoint independent third parties to act as Registration Authorities under an Entrust Certification Authority. Such independent third-party Registration Authorities shall be responsible for their performance under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust shall not be responsible for the performance of such independent third-party Registration Authorities. Independent third-party Registration Authorities may use one or more representatives or agents to perform their obligations when acting as a Registration Authority under an Entrust Certification Authority. Independent

third-party Registration Authorities shall remain responsible for the performance of such representatives or agents under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust may appoint Resellers and Co-marketers for (i) Entrust Certificates, and (ii) services provided in respect to Entrust Certificates. Such Resellers and Co-marketers shall be responsible for their performance under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Entrust shall not be responsible for the performance of any such Resellers and Co-marketers. Resellers and Co-marketers may use one or more representatives or agents to perform their obligations under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Resellers and Co-marketers shall remain responsible for the performance of such representatives or agents under the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements. Independent third-party Registration Authorities, Resellers, and Co-marketers shall be entitled to receive all of the benefit of all (i) disclaimers of representations, warranties, and conditions, (ii) limitations of liability, (iii) representations and warranties from Applicants, Subscribers, and Relying Parties, and (iv) indemnities from Applicants, Subscribers, and Relying Parties, set forth in this Entrust CPS, any Subscription Agreements, and any Relying Party Agreements.

2.1.3 Subscriber Obligations

Subscribers and Applicants shall:

(i) understand and, if necessary, receive proper education in the use of Public-Key cryptography and Certificates including Entrust Certificates;
(ii) provide, in any communications with Entrust or an independent third-party Registration Authority, correct information with no errors, misrepresentations, or omissions;
(iii) provide verification information that Entrust may request, within the time period requested;
(iv) generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Entrust Certificate or Applicant's Entrust Certificate Application, if not generated by an Entrust Certification Authority;
(v) understand and accept the risk of using a Key Pair that is less than 2048 bit RSA;
(vi) read and agree to all terms and conditions of the Entrust CPS and Subscription Agreement;
(vii) refrain from modifying the contents of an Entrust Certificate;
(viii) use Entrust Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the Entrust CPS and applicable laws including, without limitation, laws relating to import, export, data protection and the right to include personal information in Entrust Certificates;
(ix) only use an Entrust Certificate on behalf of the person, entity, or organization listed as the Subject in such Entrust Certificate;
(x) keep confidential and properly protect the Subscriber's or Applicant's Private Keys;
(xi) notify Entrust or, if Applicant submitted its Entrust Certificate Application to an independent third-party Registration Authority, such independent third-party Registration Authority, as soon as reasonably practicable of any change to any information included in the Applicant's Entrust Certificate Application or any change in any circumstances that would make the information in the Applicant's Entrust Certificate Application misleading or inaccurate;
(xii) notify Entrust or, if Subscriber received its Entrust Certificate through an independent third-party Registration Authority, such independent third-party Registration Authority, as soon as reasonably practicable of any change to any information included in the Subscriber's Entrust Certificate or any change in any circumstances that would make the information in the Subscriber's Entrust Certificate misleading or inaccurate;
(xiii) immediately cease to use an Entrust Certificate if any information included in the Subscriber's Entrust Certificate or if a change in circumstances would make the information in the Subscriber's Entrust Certificate misleading or inaccurate;
(xiv) notify Entrust or, if Subscriber received its Entrust Certificate from an independent third-party Registration Authority, such independent third-party Registration Authority, immediately of any suspected or actual Compromise of the Subscriber's or Applicant's Private Keys and request the revocation of such Entrust Certificate;

(xv) immediately cease to use the Subscriber's Entrust Certificate upon (a) expiration or revocation of such Entrust Certificate, or (b) any suspected or actual Compromise of the Private Key corresponding to the Public Key in such Entrust Certificate, and remove such Entrust Certificate from the devices and/or software in which it has been installed, where applicable;

(xvi) refrain from using the Subscriber's Private Key corresponding to the Public Key in the Subscriber's Entrust Certificate to sign other Certificates; and

(xvii) use the Subscriber's or Applicant's own judgment about whether it is appropriate, given the level of security and trust provided by an Entrust Certificate, to use an Entrust Certificate in any given circumstance.

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

2.1.3.1 Subscriber and Applicant Representations and Warranties

Subscribers and Applicants represent and warrant to Entrust and to all Certificate Beneficiaries, that:

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

(ii) provision of verification information reasonably requested by Entrust or its delegate will not be unreasonably delayed;

(iii) the Private Key corresponding to the Public Key submitted to Entrust in connection with an Entrust Certificate Application was created using sound cryptographic techniques, if not generated by an Entrust Certification Authority;

(iv) all measures necessary 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;

(v) any information provided to Entrust or to any independent third-party Registration Authorities in connection with an Entrust Certificate Application 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;

(vi) the Entrust Certificate(s) will not be installed or used until it has reviewed and verified the accuracy of the data in each Certificate;

(vii) Subscriber will immediately respond to Entrust's instructions concerning (1) compromise of the Private Key associated with any Entrust Certificate and (2) misuse or suspected misuse of an Entrust Certificate;

(viii) all use of the Entrust Certificate and its associated Private Key shall cease immediately, and the Subscriber shall promptly notify Entrust and request the revocation of the Entrust Certificate, if (1) any information included in the Entrust Certificate changes, is or becomes incorrect or inaccurate, or if any change in any circumstances would make the information in the Entrust Certificate Application or Entrust 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 Entrust Certificate;

(ix) all use of the (1) Entrust Certificate and (2) Private Key associated with the Public Key in such Entrust Certificate shall cease upon expiration or revocation of such Entrust Certificate

and such Entrust Certificate shall be removed from the devices and/or software in which it has been installed;

(x) the Entrust Certificates will not be used for any hazardous or unlawful (including tortious) activities; and

(xi) the subject named in the Entrust Certificate corresponds to the Subscriber, and that it legally exists as a valid entity in the jurisdiction of incorporation specified in the Entrust Certificates;

Entrust SSL Certificates

Subscribers and Applicants represent and warrant to Entrust and to all Certificate Beneficiaries, that:

(xii) the Entrust Certificate shall be installed only on the server accessible at the domain name listed in the Entrust Certificate, and will only be used in compliance with all applicable laws, solely for authorized company business, and solely in accordance with the Subscription Agreement and the CPS;

(xiii) the Subscriber has the exclusive right to use the domain name listed in the Entrust Certificate;

Entrust Code Signing Certificates

Subscribers and Applicants represent and warrant to Entrust and to all Certificate Beneficiaries, that:

(xiv) The information provided for applications signed using an Entrust Code Signing Certificate such as, but not limited to, application name, information URL, and application description, shall be truthful, accurate and non-misleading;

(xv) Subscriber shall not use the Entrust Code Signing Certificate to digitally sign hostile code, including spyware or other malicious software (malware) that is downloaded without user consent and Subscriber acknowledges that Entrust will revoke such Entrust Code Signing Certificate if Subscriber fails to comply;

(xvi) All use of the Entrust Code Signing Certificate and its associated Private Key shall cease immediately, and the Subscriber shall immediately notify Entrust and request the revocation of the Entrust Code Signing Certificate, if there is evidence that the Entrust Code Signing Certificate was used to digitally sign hostile or suspect code, including spyware or other malicious software (malware) or the code has a serious vulnerability;

(xvii) Subscriber will as a best practice, timestamp the digital signature after digitally signing Subscriber's code;

(xviii) Subscriber acknowledges that Application Software Vendor's may independently determine that an Entrust Code Signing Certificate is being used for malicious purposes or has been compromised and that such Application Software Vendor and Application Software Vendor products may have the ability to modify its customer experiences or "blacklist" an Entrust Code Signing Certificate without notice to Subscriber or Entrust and without regard to the revocation status of the Entrust Code Signing Certificate; and

(xix) Subscriber acknowledges that (a) Entrust will not provide Entrust Code Signing Certificates with signing keys that are less than 2048 bits, and (b) Entrust will hash the Entrust Code Signing Certificate with the SHA-2 algorithm unless the Subscriber requests the SHA-1 algorithm to sign code for Windows Vista or Windows Server 2008.

Entrust Document Signing Certificates

Subscribers and Applicants represent and warrant to Entrust and to all Certificate Beneficiaries, that:

(xx) Document Signing Certificate Key Pair shall be generated in a cryptographic module that prevents exportation or duplication and that meets or exceed the requirements as defined in §6.8

Entrust Time-Stamp Certificates

Subscribers and Applicants represent and warrant to Entrust and to all Certificate Beneficiaries, that:

(xxi) Subscriber shall use the Time-Stamp Certificate for time-stamping services only. All time-stamps must be accurate and the Subscriber accepts responsibility for any inaccuracies.

(xxii) Time-Stamp Certificate Key Pair shall be generated in a cryptographic module that prevents exportation or duplication and that meets or exceed the requirements as defined in §6.8

2.1.3.2 Subscriber Notice Requirements

No stipulation.

2.1.4 Relying Party Obligations

Relying Parties shall:

(i) understand and, if necessary, receive proper education in the use of Public-Key cryptography and Certificates including Entrust Certificates;

(ii) read and agree to all terms and conditions of the Entrust CPS and the Relying Party Agreement;

(iii) verify Entrust Certificates, including use of CRLs, in accordance with the certification path validation procedure specified in ITU-T Rec. X.509:2005 | ISO/IEC 9594-8 (2005), taking into account any critical extensions and approved technical corrigenda as appropriate;

(iv) understand and accept the risk of connecting to a secure server whose Key Pair is less than 2048 bits RSA; and

(iv) make their own judgment and rely on an Entrust Certificate only if such reliance is reasonable in the circumstances, including determining whether such reliance is reasonable given the nature of the security and trust provided by an Entrust Certificate and the value of any transaction that may involve the use of an Entrust Certificate.

Entrust SSL Certificates

Relying Parties shall:

(v) trust and make use of an Entrust SSL Certificate only if the Entrust SSL Certificate has not expired or been revoked and if a proper chain of trust can be established to a trustworthy root.

Entrust Code Signing, Client and Document Signing Certificates

Relying Parties shall:

(vi) trust and make use of a digital signature created using the Private Key corresponding to the Public Key listed in the Entrust Certificate only if the Entrust Certificate was not expired or revoked at the time the digital signature was created and if a proper chain of trust can be established to a trustworthy root.

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

2.1.4.1 Relying Party Representations and Warranties

Relying Parties represent and warrant to Entrust that:

(i) the Relying Party shall properly validate an Entrust Certificate before making a determination about whether to rely on such Entrust Certificate, including confirmation that the Entrust Certificate has not expired or been revoked and that a proper chain of trust can be established to a trustworthy root;

(ii) the Relying Party shall not rely on an Entrust Certificate that cannot be validated back to a trustworthy root;

(iii) the Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on an Entrust Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by an Entrust

Certificate and the value of any transaction that may involve the use of an Entrust Certificate; and

(iv) the Relying Party shall not use an Entrust Certificate for any hazardous or unlawful (including tortious) activities.

Entrust SSL Certificates

Relying Parties represent and warrant to Entrust that:

(v) the Relying Party shall not rely on a revoked or expired Entrust SSL Certificate;

Entrust Code Signing, Client, Document Signing, and Time-Stamp Certificates

Relying Parties represent and warrant to Entrust that:

(vi) the Relying Party shall not rely on a digital signature created using the Private Key corresponding to the Public Key listed in the Entrust Certificate if the Entrust Certificate was expired at the time the digital signature was created or if the Certificate is revoked.

2.1.5 Repository Obligations

An Entrust Repository shall:

(i) make available, in accordance with the terms and conditions of the Entrust CPS, Entrust Certificate revocation information published by an Entrust Certification Authority; and

(ii) make available a copy of the Entrust CPS and other information related to the products and services provided by Entrust Certification Authorities and any Registration Authorities operating under the Entrust Certification Authorities.

2.2 Liability

THE MAXIMUM CUMULATIVE LIABILITY OF THE ENTRUST GROUP TO ANY APPLICANTS, SUBSCRIBERS, RELYING PARTIES OR ANY OTHER PERSONS, ENTITIES, OR ORGANIZATIONS FOR ANY LOSSES, COSTS, EXPENSES, LIABILITIES, DAMAGES, CLAIMS, OR SETTLEMENT AMOUNTS ARISING OUT OF OR RELATING TO USE OF AN ENTRUST CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO ANY ENTRUST CERTIFICATES IS LIMITED BY THIS ENTRUST CPS. THIS ENTRUST CPS ALSO CONTAINS LIMITED WARRANTIES, LIMITATIONS ON LIABILITY, AND DISCLAIMERS OF REPRESENTATIONS, WARRANTIES AND CONDITIONS.

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

Entrust makes the following limited warranties to Subscribers with respect to the operation of Entrust Certification Authorities:

(i) Entrust Certification Authorities shall provide Repository services consistent with the practices and procedures set forth in this Entrust CPS;

(ii) Entrust Certification Authorities shall perform Entrust Certificate issuance consistent with the procedures set forth in this Entrust CPS; and

(iii) Entrust Certification Authorities shall provide revocation services consistent with the procedures set forth in this Entrust CPS.

Notwithstanding the foregoing, in no event does the Entrust Group make any representations, or provide any warranties, or conditions to any Applicants, Subscribers, Relying Parties, or any other persons, entities, or organizations with respect to (i) the techniques used in the generation and storage of the Private Key corresponding to the Public Key in an Entrust Certificate, including, whether such Private Key has been Compromised or was generated using sound cryptographic techniques, (ii) the reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing an Entrust Certificate, (iii) any software whatsoever, or (iv) non-repudiation of any Entrust Certificate or any transaction facilitated through the use of an Entrust Certificate, since such determination is a matter of applicable law.

Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to Entrust Certificates and Entrust Certificate Applications are dependent on the transmission of information over communication infrastructures such as, without limitation, the Internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges ("Telecommunication Equipment") and that this Telecommunication Equipment is not under the control of Entrust. The Entrust Group shall not be liable for any error, failure, delay, interruption, defect, or corruption in relation to an Entrust Certificate, an Entrust Certificate CRL, Entrust OCSP message, or an Entrust Certificate Application to the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

2.2.1.2 Disclaimers

EXCEPT AS SPECIFICALLY PROVIDED IN SECTION 2.2.1.1, THE ENTRUST GROUP DOES NOT MAKE ANY REPRESENTATIONS OR GIVE ANY WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND THE ENTRUST GROUP SPECIFICALLY DISCLAIMS ANY AND ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SATISFACTORY QUALITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE.

2.2.1.3 Loss Limitations

THE ENTRUST GROUP'S ENTIRE LIABILITY UNDER THE ENTRUST CPS IS SET FORTH IN THE APPLICABLE SUBSCRIPTION AGREEMENT(S) AND/OR RELYING PARTY AGREEMENT(S). THE ENTRUST GROUP'S ENTIRE LIABILITY TO ANY OTHER PARTY IS SET OUT IN THE AGREEMENT(S) BETWEEN ENTRUST AND SUCH OTHER PARTY. TO THE EXTENT ENTRUST HAS ISSUED THE ENTRUST CERTIFICATE IN COMPLIANCE WITH THE ENTRUST CPS, THE ENTRUST GROUP SHALL HAVE NO LIABILITY TO THE SUBSCRIBER, RELYING PARTY OR ANY OTHER PARTY FOR ANY CLAIMS, DAMAGES OR LOSSES SUFFERED AS THE RESULT OF THE USE OF OR RELIANCE ON SUCH ENTRUST CERTIFICATE.

FOR GREATER CERTAINTY, ENTRUST GROUP'S ENTIRE LIABILITY UNDER THIS ENTRUST CPS TO: (I) AN APPLICANT OR SUBSCRIBER IS SET OUT IN THE SUBSCRIPTION AGREEMENT BETWEEN ENTRUST (OR AN AFFILIATE OF ENTRUST) AND SUCH SUBSCRIBER; AND (II) A RELYING PARTY IS SET OUT IN THE RELYING PARTY AGREEMENT POSTED IN THE REPOSITORY ON THE DATE THE RELYING PARTY RELIES ON SUCH ENTRUST CERTIFICATE.

2.2.1.4 Other Exclusions

Without limitation, the Entrust Group shall not be liable to any Applicants, Subscribers, Relying Parties or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of an Entrust Certificate or any services provided in respect to an Entrust Certificate if:

(i) the Entrust Certificate was issued as a result of errors, misrepresentations, or other acts or omissions of a Subscriber or of any other person, entity, or organization;
(ii) the Entrust Certificate has expired or has been revoked;
(iii) the Entrust Certificate has been modified or otherwise altered;
(iv) the Subscriber failed to stop using an Entrust Certificate after the information contain in such Entrust Certificate changed or after circumstances changed so that the information contained in such Entrust Certificate became misleading or inaccurate;
(v) a Subscriber breached the Entrust CPS or the Subscriber's Subscription Agreement, or a Relying Party breached the Entrust CPS or the Relying Party's Relying Party Agreement;
(vi) the Private Key associated with the Entrust Certificate has been Compromised; or

(vii) the Entrust Certificate is used other than as permitted by the Entrust CPS or is used in contravention of applicable law.

In no event shall the Entrust Group be liable to any Applicant, Subscriber, or any other person, entity, or organization for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to the refusal by Entrust to issue or request the issuance of an Entrust Certificate. In no event shall the Entrust Group be liable to any Applicant, Subscriber, or any other person, entity, or organization for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to any delay by the Entrust Group, in issuing or in requesting the issuance of an Entrust Certificate.

In no event shall the Entrust Group be liable to any Subscriber, Relying Party, or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to any proceeding or allegation that an Entrust Certificate or any information contained in an Entrust Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates any patent, trademark, copyright, trade secret, or any other intellectual property right or other right of any person, entity, or organization in any jurisdiction.

2.2.1.5 Hazardous Activities

Entrust Certificates and the services provided by Entrust in respect to Entrust Certificates are not designed, manufactured, or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines. The Entrust Group specifically disclaims any and all representations, warranties, and conditions with respect to such uses, whether express, implied, statutory, by usage of trade, or otherwise.

2.2.2 RA Liability

The same liability provisions that apply in §2.2.1 with respect to Entrust Certification Authorities shall apply with respect to Entrust-operated Registration Authorities and independent third-party Registration Authorities operating under Entrust Certification Authorities.

2.3 Financial Responsibility

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers, Relying Parties, and to any other persons, entities, or organizations for any transactions in which such Subscribers or Relying Parties participate and which use Entrust Certificates or any services provided in respect to Entrust Certificates. Entrust makes no representations and gives no warranties or conditions regarding the financial efficacy of any transaction completed utilizing an Entrust Certificate or any services provided in respect to Entrust Certificates and the Entrust Group shall have no liability except as explicitly set forth herein in respect to the use of or reliance on an Entrust Certificate or any services provided in respect to Entrust Certificates.

2.3.1 Indemnification by Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY USE OR RELIANCE BY A RELYING PARTY ON ANY ENTRUST CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO ENTRUST CERTIFICATES, INCLUDING (I) LACK OF PROPER VALIDATION OF AN ENTRUST CERTIFICATE BY A RELYING PARTY, (II) RELIANCE BY THE RELYING PARTY ON AN EXPIRED OR REVOKED ENTRUST CERTIFICATE, (III) USE OF AN ENTRUST CERTIFICATE OTHER THAN AS PERMITTED BY THE ENTRUST CPS, THE

SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A RELYING PARTY TO EXERCISE REASONABLE JUDGMENT IN THE CIRCUMSTANCES IN RELYING ON AN ENTRUST CERTIFICATE, OR (V) ANY CLAIM OR ALLEGATION THAT THE RELIANCE BY A RELYING PARTY ON AN ENTRUST CERTIFICATE OR THE INFORMATION CONTAINED IN AN ENTRUST CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, RELYING PARTIES SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERT'S FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

2.3.1.1 Indemnification by Subscribers

SUBSCRIBERS SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY RELIANCE BY A RELYING PARTY ON ANY ENTRUST CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO ENTRUST CERTIFICATES, INCLUDING ANY (I) ERROR, MISREPRESENTATION OR OMISSION MADE BY A SUBSCRIBER IN USING OR APPLYING FOR AN ENTRUST CERTIFICATE, (II) MODIFICATION MADE BY A SUBSCRIBER TO THE INFORMATION CONTAINED IN AN ENTRUST CERTIFICATE, (III) USE OF AN ENTRUST CERTIFICATE OTHER THAN AS PERMITTED BY THE ENTRUST CPS, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A SUBSCRIBER TO TAKE THE NECESSARY PRECAUTIONS TO PREVENT LOSS, DISCLOSURE, COMPROMISE OR UNAUTHORIZED USE OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY IN SUCH SUBSCRIBER'S ENTRUST CERTIFICATE, OR (V) ALLEGATION THAT THE USE OF A SUBSCRIBER'S ENTRUST CERTIFICATE OR THE INFORMATION CONTAINED IN A SUBSCRIBER'S ENTRUST CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, A SUBSCRIBER SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERTS FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

2.3.2 Fiduciary Relationships

Nothing contained in this Entrust CPS, or in any Subscription Agreement, or any Relying Party Agreement shall be deemed to constitute the Entrust Group as the fiduciary, partner, agent, trustee, or legal representative of any Applicant, Subscriber, Relying Party or any other person, entity, or organization or to create any fiduciary relationship between the Entrust Group and any Subscriber, Applicant, Relying Party or any other person, entity, or organization, for any purpose whatsoever. Nothing in the Entrust CPS, or in any

Subscription Agreement or any Relying Party Agreement shall confer on any Subscriber, Applicant, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf ofthe Entrust Group.

2.3.3 Administrative Processes

No Stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

Unless otherwise set out in in a Subscription Agreement or Relying Party Agreement, 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 Entrust CPS, all Subscription Agreements and all Relying Party Agreements. The application of the United Nations Convention on Contracts for the International Sale of Goods to the Entrust CPS, any Subscription Agreements, and any Relying Party Agreements is expressly excluded. Any dispute arising out of or in respect to the Entrust CPS, any Subscription Agreement, any Relying Party Agreement, or in respect to any Entrust Certificates or any services provided in respect to any Entrust Certificates that is not resolved by alternative dispute resolution, shall be brought in the provincial or federal courts sitting in Ottawa, Ontario, and each person, entity, or organization 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, Applicants, Subscribers, and Relying Parties waive any right that such Applicants, Subscribers, and Relying Parties may have to a jury trial.

2.4.1.1 Force Majeure

The Entrust Group shall not be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms of the Entrust CPS, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Entrust is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.

2.4.1.2 Interpretation

All references in this Entrust CPS to "Sections" refer to the sections of this Entrust CPS. As used in this Entrust CPS, neutral pronouns and any variations thereof shall be deemed to include the feminine and masculine and all terms used in the singular shall be deemed to include the plural, and vice versa, as the context may require. The words "hereof", "herein", and "hereunder" and other words of similar import refer to this Entrust CPS as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this Entrust CPS. The word "including" when used herein is not intended to be exclusive and means "including, without limitation."

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 Severability

Whenever possible, each provision of the Entrust CPS, any Subscription Agreements, and any Relying Party Agreements shall be interpreted in such a manner as to be effective and valid under applicable law. If the application of any provision of the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements or any portion thereof to any particular facts or circumstances shall 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 the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements shall not in any way be

affected or impaired thereby, and (ii) such provision shall be enforced to the maximum extent possible so as to effect its intent and it shall 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 THE ENTRUST CPS, ANY SUBSCRIPTION AGREEMENTS, OR ANY RELYING PARTY AGREEMENTS THAT DEAL 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 THE ENTRUST CPS, ANY SUBSCRIPTION AGREEMENTS, OR ANY RELYING PARTY AGREEMENTS AND SHALL BE SO INTERPRETED AND ENFORCED.

2.4.2.2 Survival

The provisions of the section entitled "Definitions" and sections 2.1.3.1, 2.1.4.1, 2.2, 2.3, 2.4, 2.8, 2.9, 3.1.5, 3.1.6, 4.6 and 8.1 shall survive termination or expiration of the Entrust CPS, any Subscription Agreements, and any Relying Party Agreements. All references to sections that survive termination of the Entrust CPS, any Subscription Agreements, and any Relying Party Agreements, shall include all sub-sections of such sections. All payment obligations shall survive any termination or expiration of the Entrust CPS, any Subscription Agreements, and any Relying Party Agreements.

2.4.2.3 Merger

The Entrust CPS, the Subscription Agreements, and the Relying Party Agreements state all of the rights and obligations of the Entrust Group, any Applicant, Subscriber, or Relying Party and any other persons, entities, or organizations in respect to the subject matter hereof and thereof and such rights and obligations shall not be augmented or derogated by any prior agreements, communications, or understandings of any nature whatsoever whether oral or written. The rights and obligations of the Entrust Group may not be modified or waived orally and may be modified only in a writing signed or authenticated by a duly authorized representative of Entrust.

2.4.2.4 Conflict of Provisions

In the event of any inconsistency between the provisions of this Entrust CPS and the provisions of any Subscription Agreement or any Relying Party Agreement, the terms and conditions of this Entrust CPS shall govern.

2.4.2.5 Waiver

The failure of Entrust to enforce, at any time, any of the provisions of this Entrust CPS, a Subscription Agreement with Entrust, or a Relying Party Agreement with Entrust or the failure of Entrust to require, at any time, performance by any Applicant, Subscriber, Relying Party or any other person, entity, or organization of any of the provisions of this Entrust CPS, a Subscription Agreement with Entrust, or a Relying Party Agreement with Entrust, shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of Entrust to enforce each and every such provision thereafter. The express waiver by Entrust of any provision, condition, or requirement of this Entrust CPS, a Subscription Agreement with Entrust, or a Relying Party Agreement with Entrust shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement. The failure of an independent third-party Registration Authority or Reseller operating under an Entrust Certification Authority ("Registration Authority") to enforce, at any time, any of the provisions of a this Entrust CPS, any Subscription Agreement with such Registration Authority, or any Relying Party Agreement with such Registration Authority or the failure to require by such Registration Authority, at any time, performance by any Applicant, Subscriber, Relying Party or any other person, entity, or organization of this Entrust CPS, any Subscription Agreement with such Registration Authority, or any Relying Party Agreement with such Registration Authority shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of such Registration Authority to enforce each and every such provision thereafter. The express waiver by a Registration Authority of any provision, condition, or requirement of a

Subscription Agreement with such Registration Authority or a Relying Party Agreement with such Registration Authority shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

2.4.2.6 Notice

Any notice to be given by a Subscriber, Applicant, or Relying Party to Entrust under this Entrust CPS, a Subscription Agreement, or a Relying Party Agreement shall be given in writing to the address specified in §1.4 by prepaid receipted mail, facsimile, or overnight courier, and shall be effective as follows (i) in the case of facsimile or courier, on the next Business Day, and (ii) in the case of receipted mail, five (5) Business Days following the date of deposit in the mail. Any notice to be given by Entrust under the Entrust CPS, any Subscription Agreement, or any Relying Party Agreement shall be given by email or by facsimile or courier to the last address, email address or facsimile number for the Subscriber on file with Entrust. In the event of notice by email, the notice shall become effective on the next Business Day. In the event of notice by prepaid receipted mail, facsimile, or overnight courier, notice shall become effective as specified in (i) or (ii), depending on the means of notice utilized.

2.4.2.7 Assignment

Entrust Certificates and the rights granted under the Entrust CPS, any Subscription Agreement, or any Relying Party Agreement are personal to the Applicant, Subscriber, or Relying Party that entered into the Subscription Agreement or Relying Party Agreement and cannot be assigned, sold, transferred, or otherwise disposed of, whether voluntarily, involuntarily, by operation of law, or otherwise, without the prior written consent of Entrust or the Registration Authority under an Entrust Certification Authority with which such Applicant, Subscriber, or Relying Party has contracted. Any attempted assignment or transfer without such consent shall be void and shall automatically terminate such Applicant's, Subscriber's or Relying Party's rights under the Entrust CPS, any Subscription Agreement, or any Relying Party Agreement. Entrust may assign, sell, transfer, or otherwise dispose of the Entrust CPS, any Subscription Agreements, or any Relying Party Agreements together with all of its rights and obligations under the Entrust CPS, any Subscription Agreements, and any Relying Party Agreements (i) to an Affiliate, or (ii) as part of a sale, merger, or other transfer of all or substantially all the assets or stock of the business of Entrust to which the Entrust CPS, the Subscription Agreements, and Relying Party Agreements relate. Subject to the foregoing limits, this Agreement shall be binding upon and shall inure to the benefit of permitted successors and assigns of Entrust, any third-party Registration Authorities operating under the Entrust Certification Authorities, Applicants, Subscribers, and Relying Parties, as the case may be.

2.4.3 Dispute Resolution Procedures

Any disputes between a Subscriber or an Applicant and Entrust or any third-party Registration Authorities operating under the Entrust Certification Authorities, or a Relying Party and Entrust or any third-party Registration Authorities operating under the Entrust Certification Authorities, shall be submitted to mediation in accordance with the Commercial Mediation Rules of the American Arbitration Association which shall take place in English in Ottawa, Ontario. In the event that a resolution to such dispute cannot be achieved through mediation within thirty (30) days, the dispute shall be submitted to binding arbitration. The arbitrator shall have the right to decide all questions of arbitrability. The dispute shall be finally settled by arbitration in accordance with the rules of the American Arbitration Association, as modified by this provision. Such arbitration shall take place in English in Ottawa, Ontario, before a sole arbitrator appointed by the American Arbitration Association (AAA) who shall be appointed by the AAA from its Technology Panel and shall be reasonably knowledgeable in electronic commerce disputes. The arbitrator shall apply the laws of the Province of Ontario, without regard to its conflict of laws provisions, and shall render a written decision within thirty (30) days from the date of close of the arbitration hearing, but no more than one (1) year from the date that the matter was submitted for arbitration. The decision of the arbitrator shall be binding and conclusive and may be entered in any court of competent jurisdiction. In each arbitration, the prevailing party shall be entitled to an award of all or a portion of its costs in such arbitration, including reasonable attorney's fees actually incurred. Nothing in the Entrust CPS, or in any Subscription Agreement, or any Relying Party Agreement shall preclude Entrust or any third-party Registration Authorities operating under the Entrust Certification Authorities from applying to any court of competent jurisdiction for

temporary or permanent injunctive relief, without breach of this §2.4.3 and without any abridgment of the powers of the arbitrator, with respect to any (i) alleged Compromise that affects the integrity of an Entrust Certificate, or (ii) alleged breach of the terms and conditions of the Entrust CPS, any Subscription Agreement, or any Relying Party Agreement. The institution of any arbitration or any action shall not relieve an Applicant, Subscriber or Relying Party of its obligations under the Entrust CPS, any Subscription Agreement, or any Relying Party Agreement.

2.4.3.1 Limitation Period on Arbitrations and Actions

Any and all arbitrations or legal actions in respect to a dispute that is related to an Entrust Certificate or any services provided in respect to an Entrust Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the Entrust Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the Entrust Certificate in dispute, whichever is sooner. If any arbitration or action in respect to a dispute that is related to an Entrust Certificate or any service or services provided in respect to an Entrust Certificate is not commenced prior to such time, any party seeking to institute such an arbitration or action shall be barred from commencing or proceeding with such arbitration or action.

2.5 Fees

The fees for services provided by Entrust in respect to Entrust Certificates are set forth in the Entrust Repository. These fees are subject to change, and any such changes shall become effective immediately after posting in the Entrust Repository. The fees for services provided by independent third-party Registration Authorities, Resellers and Co-marketers in respect to Entrust Certificates are set forth on the web sites operated by such Registration Authorities, Resellers and Co-marketers. These fees are subject to change, and any such changes shall become effective immediately after posting in such web sites.

2.5.1 Certificate Issuance or Renewal Fees

See the Entrust Repository for the fees charged by Entrust. See the web sites operated by Registration Authorities operating under the Entrust Certification Authorities, Resellers, and Co-marketers for the fees charged by such Registration Authorities, Resellers, and Co-marketers.

2.5.2 Certificate Access Fees

See the Entrust Repository for the fees charged by Entrust. See the web sites operated by Registration Authorities operating under the Entrust Certification Authorities, Resellers, and Co-marketers for the fees charged by such Registration Authorities, Resellers, and Co-marketers.

2.5.3 Revocation or Status Information Access Fees

See the Entrust Repository for the fees charged by Entrust. See the web sites operated by Registration Authorities operating under the Entrust Certification Authorities, Resellers, and Co-marketers for the fees charged by such Registration Authorities, Resellers, and Co-marketers.

2.5.4 Fees for Other Services such as Policy Information

See the Entrust Repository for the fees charged by Entrust. See the web sites operated by Registration Authorities operating under the Entrust Certification Authorities, Resellers, and Co-marketers for the fees charged by such Registration Authorities, Resellers, and Co-marketers.

2.5.5 Refund Policy

Neither Entrust nor any Registration Authorities operating under the Entrust Certification Authorities nor any Resellers or Co-Marketers provide any refunds for Entrust Certificates or services provided in respect to Entrust Certificates.

2.6 Publication and Repositories

Entrust maintains the Entrust Repository to store various information related to Entrust Certificates and the operation of Entrust Certification Authorities, Entrust Registration Authorities, and third-party Registration Authorities operating under the Entrust Certification Authorities. The Entrust CPS and various other related information is published in the Entrust Repository. The Entrust CPS is also available from Entrust in hard copy upon request.

2.6.1 Publication of CA Information

The following Entrust Certificate information is published in the Entrust Repository:

(i) the Entrust CPS;
(ii) information and agreements regarding the subscription for and reliance on Entrust Certificates; and
(iii) revocations of Entrust Certificates performed by an Entrust Certification Authority, published in a Certificate Revocation List (CRL).

The data formats used for Entrust Certificates and for Certificate Revocation Lists in the Entrust Repository are in accordance with the associated definitions in §7.

2.6.2 Frequency of Publication

The Entrust CPS may be re-issued and published in accordance with the policy set forth in §8.

2.6.3 Access Controls

The Entrust CPS is published in the Entrust Repository. The Entrust CPS will be available to all Applicants, Subscribers and Relying Parties, but may only be modified by the Entrust Policy Authority.

2.6.4 Repositories

The Entrust Certification Authorities maintain the Entrust Repositories to allow access to Entrust Certificate-related and CRL information. The information in the Entrust Repositories is accessible through a web interface and is periodically updated as set forth in this Entrust CPS. The Entrust Repositories are the only approved source for CRL and other information about Entrust Certificates.

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

Entrust Certification Authorities, Entrust-operated Registration Authorities, and independent third-party Registration Authorities operating under the Entrust Certification Authorities shall be audited once per calendar year for compliance with the practices and procedures set forth in the Entrust CPS. If the results of an audit report recommend remedial action, Entrust or the applicable independent third-party Registration Authority shall initiate corrective action within thirty (30) days of receipt of such audit report.

2.7.2 Identity/Qualifications of Auditor

The compliance audit of Entrust Certification Authorities shall be performed by a certified public accounting firm with a demonstrated competency in the evaluation of Certification Authorities and Registration Authorities.

2.7.3 Auditor's Relationship to Audited Party

The certified public accounting firm selected to perform the compliance audit for the Entrust Certification Authorities, Entrust-operated Registration Authorities, or independent third-party operated Registration Authorities under the Entrust Certification Authorities shall be independent from the entity being audited.

2.7.4 Topics Covered by Audit

The compliance audit shall test compliance of Entrust Certification Authorities, Entrust-operated Registration Authorities, or independent third-party operated Registration Authorities under the Entrust Certification Authorities against the policies and procedures set forth in:

i. the Entrust CPS; and
ii. the WebTrust Program for Certification Authorities.

2.7.5 Actions Taken as a Result of Deficiency

Upon receipt of a compliance audit that identifies any deficiencies, the audited Entrust Certification Authority, Entrust-operated Registration Authority, or independent third-party operated Registration Authority under an Entrust Certification Authority shall use commercially reasonable efforts to correct any such deficiencies in an expeditious manner.

2.7.6 Communication of Results

The results of all compliance audits shall be communicated, in the case of Entrust Certification Authorities, to the Entrust Policy Authority, and, in the case of any Entrust-operated Registration Authorities under an Entrust Certification Authorities, to the Entrust Policy Authority, and in the case of third-party Registration Authorities operating under an Entrust Certification Authority, to the operational authority for such Registration Authority.

The results of the most recent compliance audit will be posted to the Repository.

2.8 Confidentiality

Neither Entrust nor any independent third-party Registration Authorities operating under the Entrust Certification Authorities, nor any Resellers or Co-Marketers shall disclose or sell Applicant or Subscriber names (or other information submitted by an Applicant or Subscriber when applying for an Entrust Certificate), except in accordance with this Entrust CPS, a Subscription Agreement, or a Relying Party Agreement. Entrust and all independent third-party Registration Authorities operating under the Entrust Certification Authorities, and all Resellers and Co-Marketers shall use a commercially reasonable degree of care to prevent such information from being used or disclosed for purposes other than those set forth in the Entrust CPS, a Subscription Agreement, or a Relying Party Agreement. Notwithstanding the foregoing, Applicants and Subscribers acknowledge that some of the information supplied with an Entrust Certificate Application is incorporated into Entrust Certificates and that Entrust and all independent third-party Registration Authorities operating under the Entrust Certification Authorities, and all Resellers and Co-Marketers shall be entitled to make such information publicly available.

2.8.1 Types of Information to be Kept Confidential

Information that is supplied by Applicants, Subscribers, or Relying Parties for the subscription for, use of, or reliance upon an Entrust Certificate, and which is not included in the information described in §2.8.2 below, shall be considered to be confidential. Entrust and independent third-party Registration Authorities under the Entrust Certification Authorities shall be entitled to disclose such information to any subcontractors or agents that are assisting Entrust in the verification of information supplied in Entrust Certificate Applications or that are assisting Entrust in the operation of the Entrust Certification Authorities or Entrust-operated Registration Authorities. Information considered to be confidential shall not be disclosed unless compelled pursuant to legal, judicial, or administrative proceedings, or otherwise required by law. Entrust and independent third-party Registration Authorities under the Entrust Certification Authorities shall be entitled to disclose information that is considered to be confidential to legal and financial advisors assisting in connection with any such legal, judicial, administrative, or other proceedings required by law, and to potential acquirors, legal counsel, accountants, banks and financing sources and their advisors in connection with mergers, acquisitions, or reorganizations.

2.8.2 Types of Information not Considered Confidential

Information that is included in an Entrust Certificate or a Certificate Revocation List shall not be considered confidential. Information contained in the Entrust CPS shall not be considered confidential. Without limiting the foregoing, information that (i) was or becomes known through no fault of Entrust, an independent third-party Registration Authority under an Entrust Certification Authority, a Reseller, or a Co-marketer, (ii) was rightfully known or becomes rightfully known to Entrust, an independent third-party Registration Authority under the Entrust Certification Authority, a Reseller, or a Co-marketer without confidential or proprietary restriction from a source other than the Subscriber, (iii) is independently developed by Entrust, an independent third-party Registration Authority under an Entrust Certification Authority, a Reseller, or a Co-marketer, or (iv) is approved by a Subscriber for disclosure, shall not be considered confidential.

2.8.3 Disclosure of Certificate Revocation/Suspension Information

If an Entrust Certificate is revoked by an Entrust Certification Authority, a serial number will be included in the Certificate Revocation List entry for the revoked Entrust Certificate.

2.8.4 Release to Law Enforcement Officials

Entrust, independent third-party Registration Authorities under an Entrust Certification Authority, Resellers, and Co-marketers shall have the right to release information that is considered to be confidential to law enforcement officials in compliance with applicable law.

2.8.5 Release as Part of Civil Discovery

Entrust, independent third-party Registration Authorities under an Entrust Certification Authority, Resellers, and Co-marketers may disclose information that is considered confidential during the course of any arbitration, litigation, or any other legal, judicial, or administrative proceeding relating to such information. Any such disclosures shall be permissible provided that Entrust, the independent third-party Registration Authority, Reseller, or Co-marketer uses commercially reasonable efforts to obtain a court-entered protective order restricting the use and disclosure of any such information to the extent reasonably required for the purposes of such arbitration, litigation, or any other legal, judicial, or administrative proceeding.

2.8.6 Disclosure Upon Owner's Request

Entrust, independent third-party Registration Authorities under an Entrust Certification Authority, Resellers, and Co-marketers may disclose information provided to Entrust, such Registration Authority, Reseller or Co-marketer, by an Applicant, a Subscriber, or a Relying Party upon request of such Applicant, Subscriber, or Relying Party.

2.8.7 Other Information Release Circumstances

No stipulation.

2.9 Intellectual Property Rights

Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under all Entrust Certificates, except for any information that is supplied by an Applicant or a Subscriber and that is included in an Entrust Certificate, which information shall remain the property of the Applicant or Subscriber. All Applicants and Subscribers grant to Entrust and any Registration Authorities operating under the Entrust Certification Authorities a non-exclusive, worldwide, paid-up, royalty-free license to use, copy, modify, publicly display, and distribute such information, by any and all means and through any and all media whether now known or hereafter devised for the purposes contemplated under the Entrust CPS, the Subscriber's Subscription Agreement, and any Relying Party Agreements. Entrust and any Registration Authorities operating under the Entrust Certification Authorities shall be entitled to transfer, convey, or assign this license in conjunction with any transfer, conveyance, or assignment as contemplated in §2.4.2.7. Entrust grants to Subscribers and Relying Parties a non-exclusive, non-transferable license to use, copy, and distribute Entrust Certificates, subject to such Entrust Certificates being used as contemplated under the Entrust CPS, the Subscriber's Subscription Agreement, and any Relying Party Agreements, and further

provided that such Entrust Certificates are reproduced fully and accurately and are not published in any publicly available database, repository, or directory without the express written permission of Entrust. Except as expressly set forth herein, no other right is or shall be deemed to be granted, whether by implication, estoppel, inference or otherwise. Subject to availability, Entrust may in its discretion make copies of one or more Cross Certificate(s) available to Subscribers for use solely with the Entrust Certificate issued to such Subscribers. Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under the Cross Certificate(s).

Entrust grants permission to reproduce the Entrust CPS provided that (i) the copyright notice on the first page of this Entrust CPS is retained on any copies of the Entrust CPS, and (ii) the Entrust CPS is reproduced fully and accurately. Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under the Entrust CPS.

In no event shall the Entrust Group be liable to any Applicants, Subscribers, or Relying Parties or any other third parties for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising from or relating to claims of infringement, misappropriation, dilution, unfair competition, or any other violation of any patent, trademark, copyright, trade secret, or any other intellectual property or any other right of person, entity, or organization in any jurisdiction arising from or relating to any Entrust Certificate or arising from or relating to any services provided in relation to any Entrust Certificate.

3 Identification and Authentication

3.1 Initial Registration

Before issuing an Entrust Certificate, the Entrust Certification Authorities ensure that all Subject organization information in the Entrust Certificate conforms to the requirements of, and has been verified in accordance with the procedures prescribed in this CPS and matches the information confirmed and documented by the Registration Authority pursuant to its verification processes.

3.1.1 Types of Names

Entrust SSL Certificates

The Subject names in an Entrust SSL Certificate comply with the X.501 Distinguished Name (DN) form. Entrust Certification Authorities shall use a single naming convention as set forth below. Each Entrust SSL Certificate shall contain the following information:

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located and plans to host the secure server on which the Applicant is intending to install the Entrust SSL Certificate;
(ii) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship, the organization name can be the name of the Applicant;
(iii) "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, marketing, and development);
(iv) "Common Name" (CN) which is the hostname, the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the Entrust SSL Certificate;
(v) "State" (ST), which is the state or province of the organization's place of business, if applicable; and
(vi) "Subject Alternative Name" (SAN), which is the hostname, the fully qualified hostname or path used in the DNS of the secure server on which the Applicant is intending to install the Entrust SSL Certificate. There may be multiple SANs in each Entrust SSL Certificate.

Entrust Code Signing Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;
(ii) "Organization Name" (O) which is the full legal name of the organization;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which is the same value as the "Organization Name";
(v) "Locality" (L), which is the city or locality of the organization's place of business; and
(vi) "State" (ST), which is the state or province of the organization's place of business, if applicable

Entrust Class 1 Client Certificates

(i) "Common Name" (CN) which is the e-mail address of the Subscriber;
(ii) "Email" (E), which is the e-mail address of the Subscriber; and
(iii) "Subject Alternative Name" (SAN), which is the e-mail address of the Subscriber.

Entrust Class 2 Client Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;
(ii) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship or individual, the organization name is not required, but may be the name of the Applicant;

(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which is the name of the Subscriber and is a natural person;
(v) "Email" (E), which is the e-mail address of the Subscriber; and
(vi) "Subject Alternative Name" (SAN), which is the e-mail address of the Subscriber.

Entrust Document Signing Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;
(ii) "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship or individual, the organization name is not required, but may be the name of the Applicant;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which may be an individual's name, an organization's name or the name of a specific role within an organization.

Entrust Time-Stamp Certificates

(i) "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located;
(ii) "Organization Name" (O) which is the full legal name of the organization;
(iii) "Organizational Unit Name" (OU) which is an optional field;
(iv) "Common Name" (CN) which is an optional field;
(v) "Locality" (L), which is the city or locality of the organization's place of business; and
(vi) "State" (ST), which is the state or province of the organization's place of business, if applicable

3.1.2 Need for Names to Be Meaningful

The certificates issued pursuant to this CPS are meaningful only if the names that appear in the certificates can be understood and used by Relying Parties. Names used in the certificates must identify the person or object to which they are assigned in a meaningful way. CAs shall not issue certificates to the subscribers that contain domain names, IP addresses, DN, URL, and/or e-mail addresses that the subscribers do not legitimately own or control. Examples of fields and extensions where these names appear include subject DN and subject alternative names.

Application Note: Above general prohibition naturally also covers the case when the certificate can be used for Man in the Middle insertion or Traffic Interception and Management.

Entrust SSL Certificates

The value of the Common Name to be used in an Entrust SSL Certificate shall be the Applicant's fully qualified hostname or path that is used in the DNS of the secure server on which the Applicant is intending to install the Entrust SSL Certificate. Notwithstanding the preceding sentence, the Common Name may include wildcard characters (i.e., an asterisk character) in Entrust's sole discretion.

Entrust Code Signing Certificates

The value of the Common Name to be used in an Entrust Code Signing Certificate shall be the Applicant's Organization Name.

Entrust Client Certificates

The value of the Common Name to be used in an Entrust Client Certificate shall be the name or the email address of the Subscriber.

Entrust Document Signing Certificates

The value of the Common Name to be used in an Entrust Document Signing Certificate shall be the name of the Subscriber, the role of the Subscriber, or the group or organization that the Subscriber represents.

Entrust Time-Stamp Certificates
The value of the Common Name to be used in an Entrust Time-Stamp, if present shall be a name of the time-stamp service associated with the Subscriber.

3.1.3 Rules for Interpreting Various Name Forms

Subject names for Entrust Certificates shall be interpreted as set forth in §3.1.1 and §3.1.2.

3.1.4 Uniqueness of Names

Names shall be defined unambiguously for each Subject in an Entrust Repository. The Distinguished Name attribute will usually be unique to the Subject to which it is issued. Each Entrust Certificate shall be issued a unique serial number within the name space of the issuing Entrust Certification Authority.

3.1.5 Name Claim Dispute Resolution Procedure

The Subject names in Entrust Certificates are issued on a "first come, first served" basis. By accepting a Subject name for incorporation into an Entrust Certificate, a Registration Authority operating under an Entrust Certification Authority does not determine whether the use of such information infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property right or any other rights of any person, entity, or organization. The Entrust Certification Authorities and any Registration Authorities operating under the Entrust Certification Authorities neither act as an arbitrator nor provide any dispute resolution between Subscribers or between Subscribers and third-party complainants in respect to the use of any information in an Entrust Certificate. The Entrust CPS does not bestow any procedural or substantive rights on any Subscriber or third-party complainant in respect to any information in an Entrust Certificate. Neither the Entrust Certification Authorities nor any Registration Authorities operating under the Entrust Certification Authorities shall in any way be precluded from seeking legal or equitable relief (including injunctive relief) in respect to any dispute between Subscribers or between Subscribers and third-party complainants or in respect to any dispute between Subscribers and an Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority or between a third-party complainant and an Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority arising out of any information in an Entrust Certificate. Entrust Certification Authorities and Registration Authorities operating under Entrust Certification Authorities shall respectively have the right to revoke and the right to request revocation of Entrust Certificates upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of an Entrust Certificate.

3.1.6 Recognition, Authentication and Role of Trademarks

An Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority may, in certain circumstances, take action in respect to an Entrust Certificate containing information that possibly violates the trademark rights of a third-party complainant. In the event that a third-party complainant provides an Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority with (i) a certified copy that is not more than three (3) months old of a trademark registration from the principal trademark office in any one of the United States, Canada, Japan, Australia or any of the member countries of the European Union, and further provided that such registration is still in full force and effect, and (ii) a copy of a prior written notice to the Subscriber of the Entrust Certificate in dispute, stating that the complainant believes that information in the Subscriber's Entrust Certificate violates the trademark rights of the complainant, and (iii) a representation by the complainant indicating the means of notice and basis for believing that such notice was received by the Subscriber of the Entrust Certificate in dispute, an Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority may initiate the following actions. The Entrust Certification Authority or the Registration Authority operating under an Entrust Certification Authority may determine whether the issue date of the Subscriber's Entrust Certificate predates the registration date on the trademark registration provided by the complainant. If the date of issuance of the Subscriber's Certificate predates the trademark registration date, the Entrust Certification Authority or the Registration Authority operating under the Entrust Certification Authority will take no further action unless presented with an authenticated order from an arbitrator or court of competent jurisdiction. If the date of issuance of the

Entrust Certificate is after the registration date on the trademark registration provided by the complainant, the Entrust Certification Authority or the Registration Authority operating under the Entrust Certification Authority shall request that the Subscriber provide a proof of ownership for the Subscriber's own corresponding trademark registration from the principal trademark office in any one of the United States, Canada, Japan, Australia or any of the member countries of the European Union. If the Subscriber can provide a certified copy, as set forth above, that predates or was issued on the same date as the complainant's trademark registration, the Entrust Certification Authority or the Registration Authority operating under the Entrust Certification Authority will take no further action unless presented with an authenticated order from an arbitrator or court of competent jurisdiction. If the Subscriber does not respond within ten (10) Business Days, or if the date on the certified copy of the trademark registration provided by the Subscriber postdates the certified copy of the trademark registration provided by the complainant, the Entrust Certification Authority and the Registration Authorities operating under that Entrust Certification Authority respectively may revoke or may request revocation of the disputed Entrust Certificate.

If a Subscriber files litigation against a complainant, or if a complainant files litigation against a Subscriber, and such litigation is related to any information in an issued Entrust Certificate, and if the party instigating the litigation provides an Entrust Certification Authority or a Registration Authority operating under an Entrust Certification Authority with a copy of the file-stamped complaint or statement of claim, the Entrust Certification Authority will maintain the current status of the Entrust Certificate or the Registration Authority operating under the Entrust Certification Authority will request that the Entrust Certification Authority maintain the current status of the Entrust Certificate, subject to any requirements to change the status of such Entrust Certificate otherwise provided or required under this Entrust CPS, a Subscription Agreement, or any Relying Party Agreement. During any litigation, an Entrust Certification Authority will not revoke and a Registration Authority operating under an Entrust Certification Authority will not request revocation of an Entrust Certificate that is in dispute unless ordered by an arbitrator or a court of competent jurisdiction or as otherwise provided or required under this Entrust CPS, a Subscription Agreement, or any Relying Party Agreement. In the event of litigation as contemplated above, Entrust Certification Authorities and Registration Authorities operating under the Entrust Certification Authorities will comply with any directions by a court of competent jurisdiction in respect to an Entrust Certificate in dispute without the necessity of being named as a party to the litigation. If named as a party in any litigation in respect to an Entrust Certificate, Entrust and/or any third party operating a Registration Authority under an Entrust Certification Authority shall be entitled to take any action that it deems appropriate in responding to or defending such litigation. Any Subscriber or Relying Party that becomes involved in any litigation in respect to an Entrust Certificate shall remain subject to all of the terms and conditions of the Entrust CPS, the Subscriber's Subscription Agreement, and the Relying Party's Relying Party Agreement.

Registration Authorities operating under an Entrust Certification Authority shall notify the Entrust Certification Authority of any disputes of which such Registration Authority is aware and which relate to any information contained in an Entrust Certificate whose issuance was requested by such Registration Authority.

3.1.7 Method to Prove Possession of Private Key

For Key Pairs generated by the Applicant, Entrust Certification Authorities perform proof of possession tests for CSRs created using reversible asymmetric algorithms (such as RSA) by validating the signature on the CSR submitted by the Applicant with the Entrust Certificate Application.

3.1.8 Authentication of Organizational Identity

Registration Authorities operating under the Entrust Certification Authorities shall perform a limited verification of any organizational identities that are submitted by an Applicant or Subscriber. Registration Authorities operating under the Entrust Certification Authorities shall determine whether the organizational identity, address, and domain name provided with an Entrust Certificate Application are consistent with information contained in third-party databases and/or governmental sources. The information and sources used for the limited verification of Entrust Certificate Applications may vary depending on the jurisdiction of the Applicant or Subscriber.

In the case of organizational identities that are not registered with any governmental sources, Registration Authorities operating under the Entrust Certification Authorities shall use commercially reasonable efforts to confirm the existence of the organization. Such commercially reasonable efforts may include site visits or third-party attestation letter. Registration Authorities operating under the Entrust Certification Authorities shall comply with all verification practices mandated by the Entrust Policy Authority.

3.1.9 Authentication of Individual Identity

Registration Authorities operating under the Entrust Certification Authorities shall use reasonable means to verify any individual identities that are submitted by an Applicant or Subscriber.

SSL Certificates

An individual identity shall be verified by using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). The copy shall be inspected for any indication of alteration or falsification.

The Applicant's address shall be verified using a trusted form of identification such as a government ID, utility bill, or bank or credit card statement. The same government-issued ID that was used to verify the Applicant's name may be relied upon.

The request shall be verified by contacting the Applicant using a phone number that was provided from a third-party.

Class 1 Client Certificates

The identity asserted in Entrust Class 1 Client Certificates is an email address that represents the Subscriber.

Class 2 Client Certificates

The identity shall be authenticated by matching the identity provided by the Applicant or Subscriber to:

(i) information residing in the database of an identity proofing service approved by Entrust, such as a major credit bureau, or
(ii) information contained in the business records or databases (e.g. employee or customer directories) of a Registration Authority approving certificates to its own affiliated individuals.

3.1.10 Authentication of Domain Name

Registration Authorities operating under the Entrust Certification Authorities shall use reasonable means to confirm the Applicant or Subscriber has control of the domain names to be included in the Entrust Certificate. The Registration Authority shall check the WHOIS record to determine who the top level domain (TLD) is registered to. The authorization to use the domain is done by contacting an authorization contact at the entity that registered the domain name or by contacting a user identified in the WHOIS record.

If contacting a user identified in the WHOIS record by email, then only the following emails addresses may be used:

(i) Supplied by the Domain Name Registrar;
(ii) Taken from the Domain Name Registrant's "registrant", "technical", or "administrative" contact information, as it appears in the Domain's WHOIS record; or;
(iii) By pre-pending a local part to a Domain Name as follows:
    a. Local part - One of the following: 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster'; and
    b. Domain Name – Formed by pruning zero or more components from the Registered Domain Name or the requested Fully-Qualified Domain Name.

3.1.11 Authentication of Email Address

Registration Authorities operating under the Entrust Certification Authorities shall use reasonable means to confirm the Applicant or Subscriber has control of the e-mail address to be included in the Entrust Certificate. The e-mail address for Entrust Client Certificates is confirmed using the e-mail through the enrollment process.

3.1.12 Accuracy of Information

To ensure the accuracy of the information and to ensure that no misleading information is included in the certificate, each verification shall be validated by a verification manager before the information can be used to issue a certificate.

3.2 Routine Rekey

Each Entrust Certificate shall contain a Certificate expiration date. The reason for having an expiration date for a Certificate is to minimize the exposure of the Key Pair associated with the Certificate. For this reason, when processing a new Entrust Certificate Application, Entrust recommends that a new Key Pair be generated and that the new Public Key of this Key Pair be submitted with the Applicant's Entrust Certificate Application. If a Subscriber wishes to continue to use an Entrust Certificate beyond the expiry date for the current Entrust Certificate, the Subscriber must obtain a new Entrust Certificate and replace the Entrust Certificate that is about to expire. Subscribers submitting a new Entrust Certificate Application will be required to complete the initial application process, as described in §4.1.

The Registration Authority that processed the Subscriber's Entrust Certificate Application shall make a commercially reasonable effort to notify Subscribers of the pending expiration of their Entrust Certificate by sending an email to the technical contact listed in the corresponding Entrust Certificate Application. Upon expiration of an Entrust Certificate, the Subscriber shall immediately cease using such Entrust Certificate and shall remove such Entrust Certificate from any devices and/or software in which it has been installed.

Entrust SSL Certificates

For Entrust SSL Certificates, the Subscriber may request a replacement certificate using an existing key pair.

3.3 Rekey After Revocation

Entrust Certification Authorities and Registration Authorities operating under Entrust Certification Authorities do not renew Entrust Certificates that have been revoked. If a Subscriber wishes to use an Entrust Certificate after revocation, the Subscriber must apply for a new Entrust Certificate and replace the Entrust Certificate that has been revoked. In order to obtain another Entrust Certificate, the Subscriber shall be required to complete the initial application process, as described in §4.1. Upon revocation of an Entrust Certificate, the Subscriber shall immediately cease using such Entrust Certificate and shall remove such Entrust Certificate from any devices and/or software in which it has been installed.

3.4 Revocation Request

A Subscriber may request revocation of their Entrust Certificate at any time provided that the Subscriber can validate to the Registration Authority that processed the Subscriber's Entrust Certificate Application that the Subscriber is the person, organization, or entity to whom the Entrust Certificate was issued. The Registration Authority shall authenticate a request from a Subscriber for revocation of their Entrust Certificate by authenticating the Subscriber or confirming authorization of the Subscriber through a reliable method of communication. Upon receipt and confirmation of such information, the Registration Authority shall then process the revocation request as stipulated in §4.4.

Subscribers, Relying Parties, Application Software Suppliers, Anti-Malware Organizations and other third parties may report Certificate misuse or other types of fraud, compromise misuse or inappropriate conduct

related to Certificates by contacting the Registration Authority or submitting notification through the online form, https://www.entrust.net/ev/misuse.cfm.

4 Operational Requirements

4.1 Certificate Application

To obtain an Entrust Certificate, an Applicant must:

(i) generate a secure and cryptographically sound Key Pair, if not generated by an Entrust Certification Authority

(ii) agree to all of the terms and conditions of the Entrust CPS and the Subscription Agreement, and

(iii) complete and submit an Entrust Certificate Application, providing all information requested by an Entrust-operated Registration Authority or by an independent third-party Registration Authority under an Entrust Certification Authority (a "Registration Authority") without any errors, misrepresentation, or omissions.

Upon an Applicant's completion of the Entrust Certificate Application and acceptance of the terms and conditions of this Entrust CPS and the Subscription Agreement, an Entrust-operated Registration Authority or an independent third-party Registration Authority operating under an Entrust Certification Authority shall follow the procedures described in §3.1.8 and §3.1.9 to perform limited verification of the information contained in the Entrust Certificate Application. If the verification performed by a Registration Authority is successful, the Registration Authority may, in its sole discretion, request the issuance to the Applicant of an Entrust Certificate from an Entrust Certification Authority. If a Registration Authority refuses to request the issuance of an Entrust Certificate, the Registration Authority shall (i) use commercially reasonable efforts to notify the Applicant by email of any reasons for refusal, and (ii) promptly refund any amounts that have been paid in connection with the Entrust Certificate Application.

In the event of successful verification of an Entrust Certificate Application, the Registration Authority shall submit a request to an Entrust Certification Authority for the issuance of an Entrust Certificate and shall notify the Applicant by email once an Entrust Certificate has been issued by the Entrust Certification Authority.

4.1.1 Certification Authority Authorization

As of September 1, 2015, Entrust Registration Authorities will check certification authority authorization (CAA) records in accordance with RFC 6844 as part of the domain verification process. Prior to this date Entrust may not check CAA records for all Entrust SSL Certificate applications.

If a CAA record exists that does not list Entrust as an authorized CA, an RA will verify the use of the domain name despite the CAA record.

4.2 Certificate Issuance

After performing limited verification of the information provided by an Applicant with an Entrust Certificate Application, a Registration Authority operating under an Entrust Certification Authority may request that an Entrust Certification Authority issue an Entrust Certificate. Upon receipt of a request from a Registration Authority operating under an Entrust Certification Authority, the Entrust Certification Authority may generate and digitally sign an Entrust Certificate in accordance with the Certificate profile described in §7.

Upon issuance of an Entrust Certificate, neither Entrust nor any independent third-party Registration Authority operating under an Entrust Certification Authority, nor any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall have any obligation to perform any ongoing monitoring, investigation, or verification of the information provided in an Entrust Certificate Application.

4.2.1 Circumstances for Certificate Renewal

In accordance with the Subscription Agreement, Entrust Certification Authorities or Registration Authorities will provide a certificate lifecycle monitoring service which will support certificate renewal.

4.2.2 Who May Request Renewal

Subscribers or Subscriber agents may request renewal of Entrust Certificates.

4.2.3 Processing Certificate Renewal Requests

Entrust Certification Authorities or Registration Authorities will process certificate renewal requests with validated verification data. Verification data which was validated within the last thirty-nine months may be used.

Entrust Certificates may be reissued using the previously accepted Public Key, if the Public Key meets the key size requirements of §6.1.5.

4.2.4 Notification of New Certificate Issuance to Subscriber

Entrust Certification Authorities or Registration Authorities will provide Entrust Certificate renewal notification to the Subscriber or Subscriber agents through an Internet link or by email.

Subscribers or Subscriber agents may request that email renewal notices are not sent for their expiring Entrust Certificates.

4.2.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.2.6 Publication of the Renewal Certificate by the CA

Entrust Certification Authorities or Registration Authorities will provide the Subscriber with an Entrust Certificate through an Internet link.

4.2.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.3 Certificate Acceptance

Once an Entrust Certificate has been generated and placed in an Entrust Repository, the Registration Authority that requested the issuance of the Entrust Certificate shall use commercially reasonable efforts to notify the Applicant by email that the Applicant's Entrust Certificate is available.

4.4 Certificate Suspension and Revocation

An Entrust Certification Authority shall revoke an Entrust Certificate after receiving a valid revocation request from a Registration Authority operating under such Entrust Certification Authority. A Registration Authority operating under an Entrust Certification Authority shall be entitled to request and may request that an Entrust Certification Authority revoke an Entrust Certificate after such Registration Authority receives a valid revocation request from the Subscriber for such Entrust Certificate. A Registration Authority operating under an Entrust Certification Authority shall be entitled to request and shall request that an Entrust Certification Authority revoke an Entrust Certificate if such Registration Authority becomes aware of the occurrence of any event that would require a Subscriber to cease to use such Entrust Certificate.

Entrust Certification Authorities do not allow the suspension of Entrust Certificates.

4.4.1 Circumstances for Revocation

An Entrust Certification Authority shall be entitled to revoke and may revoke, and a Registration Authority operating under an Entrust Certification Authority shall be entitled to request revocation of and shall request revocation of, a Subscriber's Entrust Certificate if such Entrust Certification Authority or Registration Authority has knowledge of or a reasonable basis for believing that of any of the following events have occurred:

(i) Compromise of such Entrust Certification Authority's Private Key or Compromise of a superior Certification Authority's Private Key;
(ii) breach by the Subscriber of any of the terms of the Entrust CPS or the Subscriber's Subscription Agreement;
(iii) any change in the information contained in an Entrust Certificate issued to a Subscriber;
(iv) non-payment of any Entrust Certificate fees or service fees;
(v) a determination that an Entrust Certificate was not issued in accordance with the requirements of the Entrust CPS or the Subscriber's Subscription Agreement;
(vi) the Entrust Certification Authority receives notice or otherwise become aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in an SSL Certificate, or that the Subscriber has failed to renew its domain name;
(vii) the Entrust Certification Authority receives notice or otherwise become aware that a Subscriber has been added as a denied party or prohibited person to a blacklist, or is operating from a prohibited destination under the laws of the Entrust Certification Authority's jurisdiction of operation as described in §2.4;
(viii) the Entrust Certification Authority ceases operations for any reason or the Entrust Certification Authority's right to issue Entrust Certificates expires or is revoked or terminated and the Entrust Certification Authority has not arranged for another Certification Authority to provide revocation support for the Entrust Certificates;
(ix) a Code Signing Certificate is used to digitally sign hostile code, including spyware or other malicious software (malware); or
(x) any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of an Entrust Certificate or an Entrust Certification Authority.

A Subscriber shall request revocation of their Entrust Certificate if the Subscriber has a suspicion or knowledge of or a reasonable basis for believing that of any of the following events have occurred:

(i) Compromise of the Subscriber's Private Key;
(ii) knowledge that the original Entrust Certificate request was not authorized and such authorization will not be retroactively granted;
(iii) change in the information contained in the Subscriber's Entrust Certificate;
(iv) change in circumstances that cause the information contained in Subscriber's Entrust Certificate to become inaccurate, incomplete, or misleading.

Such revocation request shall be submitted by the Subscriber to the Registration Authority that processed the Subscriber's Entrust Certificate Application. If a Subscriber's Entrust Certificate is revoked for any reason, the Registration Authority that processed the Subscriber's Entrust Certificate Application shall make a commercially reasonable effort to notify such Subscriber by sending an email to the technical and security contacts listed in the Entrust Certificate Application. Revocation of an Entrust Certificate shall not affect any of the Subscriber's contractual obligations under this Entrust CPS, the Subscriber's Subscription Agreement, or any Relying Party Agreements.

4.4.2 Who Can Request Revocation

A Subscriber may request revocation of their Entrust Certificate at any time for any reason. If a Subscriber requests revocation of their Entrust Certificate, the Subscriber must be able to validate themselves as set forth in §3.4 to the Registration Authority that processed the Subscriber's Entrust Certificate Application. The Entrust Certification Authorities shall not be required to revoke and the Registration Authorities

operating under the Entrust Certification Authorities shall not be required to request revocation of an Entrust Certificate until a Subscriber can properly validate themselves as set forth in §3.4 and §4.4.3. An Entrust Certification Authority shall be entitled to revoke and shall revoke, and a Registration Authority operating under an Entrust Certification Authority shall be entitled to request revocation of and shall request revocation of, a Subscriber's Entrust Certificate at any time for any of the reasons set forth in §4.4.1.

4.4.3 Procedure for Revocation Request

A Registration Authority operating under an Entrust Certification Authority shall authenticate a request by a Subscriber for revocation of their Entrust Certificate by verifying (i) Subscriber authentication credentials, or (ii) authorization of the Subscriber through a reliable method of communication. Upon receipt and confirmation of such information, the Registration Authority shall send a revocation request to the Entrust Certification Authority that issued such Entrust Certificate. The Entrust Certification Authority shall make all reasonable efforts to post the serial number of the revoked Entrust Certificate to a CRL in an Entrust Repository within one (1) business day of receiving such revocation request.

For Certificate revocation that is not initiated by the Subscriber, the Registration Authority that requested revocation of the Subscriber's Entrust Certificate shall make a commercially reasonable effort to notify the Subscriber by sending an email to the technical and security contacts specified in the Subscriber's Entrust Certificate Application.

4.4.4 Revocation Request Grace Period

In the case of Private Key Compromise, or suspected Private Key Compromise, a Subscriber shall request revocation of the corresponding Entrust Certificate immediately upon detection of the Compromise or suspected Compromise. Revocation requests for other required reasons shall be made as soon as reasonably practicable.

4.4.5 Circumstances for Suspension

Entrust Certification Authorities do not suspend Entrust Certificates.

4.4.6 Who Can Request Suspension

Entrust Certification Authorities do not suspend Entrust Certificates.

4.4.7 Procedure for Suspension Request

Entrust Certification Authorities do not suspend Entrust Certificates.

4.4.8 Limits on Suspension Period

Entrust Certification Authorities do not suspend Entrust Certificates.

4.4.9 CRL Issuance Frequency

Entrust Certification Authorities shall issue CRLs as follows:

(i) CRLs for Entrust Certificates issued to subordinate CAs shall be issued at least once every twelve months or with 24 hours after revoking a subordinate CA. The next CRL update shall not be more than twelve months from the last update.

(ii) CRLs for Entrust SSL Certificate, Entrust Code Signing Certificates, Entrust Client Certificates and Entrust Document Signing Certificates shall be issued at least once every seven days.

(iii) CRLs for Entrust Time-Stamp Certificates shall be issued at least once every twelve months or with 24 hours after revoking an Entrust Time-stamp Certificate. The next CRL update shall not be more than twelve months from the last update.

4.4.10 CRL Checking Requirements

A Relying Party shall check whether the Entrust Certificate that the Relying Party wishes to rely on has been revoked. A Relying Party shall check the Certificate Revocation Lists maintained in the appropriate Repository or perform an on-line revocation status check using OCSP to determine whether the Entrust Certificate that the Relying Party wishes to rely on has been revoked. In no event shall the Entrust Group be liable for any damages whatsoever due to (i) the failure of a Relying Party to check for revocation or expiration of an Entrust Certificate, or (ii) any reliance by a Relying Party on an Entrust Certificate that has been revoked or that has expired.

4.4.11 On-line Revocation/Status Checking Availability

On-line revocation/status checking of certificates is available on a continuous basis by CRL or On-line Certificate Status Protocol (OCSP).

Entrust Certification Authorities shall sign and make available OCSP as follows:

(i) OCSP responses for Entrust Certificates issued to subordinate CAs shall be issued at least once every twelve months or within 24 hours after revoking a subordinate CA.

(ii) OCSP responses for Entrust SSL Certificates, Entrust Code Signing Certificates, Entrust Client Certificate and Entrust Document Signing Certificates issued to end entities shall be issued at least once every four days. OCSP responses will have a maximum expiration time of ten days.

(iii) OCSP responses for Entrust Time-Stamp Certificates shall be issued at least once every twelve months or within 24 hours after revoking a subordinate CA.

Code Signing Certificates that have been revoked due to key compromise or issued to unauthorized person will be maintained in the Repository for at least ten years following revocation.

The on-line locations of the CRL and the OCSP response are included in the Entrust Certificate to support software applications that perform automatic certificate status checking. A Relying Party can also be check certificate revocation status directly with the Repository at http:www.entrust.net/CPS.

4.4.12 On-line Revocation Checking Requirements

Refer to §4.4.10.

4.4.13 Other Forms of Revocation Advertisements Available

No stipulation.

4.4.14 Checking Requirements For Other Forms of Revocation Advertisements

No stipulation.

4.4.15 Special Requirements Re Key Compromise

If a Subscriber suspects or knows that the Private Key corresponding to the Public Key contained in the Subscriber's Entrust Certificate has been Compromised, the Subscriber shall immediately notify the Registration Authority that processed the Subscriber's Entrust Certificate Application, using the procedures set forth in §4.4.3, of such suspected or actual Compromise. The Subscriber shall immediately stop using such Entrust Certificate and shall remove such Entrust Certificate from any devices and/or software in which such Entrust Certificate has been installed. The Subscriber shall be responsible for investigating the circumstances of such Compromise or suspected Compromise and for notifying any Relying Parties that may have been affected by such Compromise or suspected Compromise.

4.5 Security Audit Procedures

Significant security events in the Entrust Certification Authorities are automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Authentication codes are used in conjunction with the audit

trail files to protect against modification of audit logs. Audit trail files are archived periodically. All files including the latest audit trail file are moved to backup media and stored in a secure archive facility.

The Entrust Certification Authorities and all Registration Authorities operating under an Entrust Certification Authority record in detail every action taken to process an Entrust Certificate Request and to issue an Entrust Certificate, including all information generated or received in connection with an Entrust Certificate Request, and every action taken to process the Request, including time, date, and personnel involved in the action.

The foregoing record requirements include, but are not limited to, an obligation to record the following events:

(i) Entrust Certification Authority key lifecycle management events, including:
   a. Key generation, backup, storage, recovery, archival, and destruction; and
   b. Cryptographic device lifecycle management events.

(ii) Entrust Certification Authority and Entrust Certificate lifecycle management events, including:
   a. Certificate Requests, renewal and re-key requests, and revocation;
   b. All verification activities required by this CPS;
   c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
   d. Acceptance and rejection of Certificate Requests;
   e. Issuance of Entrust Certificates; and
   f. Generation of Certificate Revocation Lists (CRLs) and OCSP messages.

(iii) Security events, including:
   a. Successful and unsuccessful PKI system access attempts;
   b. PKI and security system actions performed;
   c. Security profile changes;
   d. System crashes, hardware failures, and other anomalies;
   e. Firewall and router activities; and
   f. Entries to and exits from the Entrust Certification Authority facility.

(iv) Log entries include the following elements:
   a. Date and time of entry;
   b. Identity of the person making the journal entry; and
   c. Description of entry.

The time for the Entrust Certification Authorities computer systems is synchronized with the service provided by the National Research Council Canada.

4.6 Records Archival

The audit trail files, databases and revocation information for Entrust Certification Authorities are archived. The archive of an Entrust Certification Authorities' database and the archive of revocation information are retained for at least three (3) years. Archives of audit trail files are retained for at least seven (7) year(s) after any Entrust Certificate based on that documentation ceases to be valid. The databases for Entrust Certification Authorities are encrypted and protected by Entrust software master keys. The archive media is protected through storage in a restricted-access facility to which only Entrust-authorized personnel have access. Archive files are backed up as they are created. Originals are stored on-site and housed with an Entrust Certification Authority system. Backup files are stored at a secure and separate geographic location.

4.7 Key Changeover

Entrust Certification Authorities' key pairs will be retired from service at the end of their respective lifetimes as defined in §6.3. New Certification Authority key pairs will be created as required to support the continuation of Entrust Certification Authority Services. Each Entrust Certification Authority will continue to publish CRLs signed with the original key pair until all certificates issued using that original key pair

have expired. The Certification Authority key changeover process will be performed such that it causes minimal disruption to Subscribers and Relying Parties.

4.8 Compromise and Disaster Recovery

Entrust Certification Authorities have a disaster recovery plan to provide for timely recovery of services in the event of a system outage. The disaster recovery plan addresses the following:

(i) the conditions for activating the plans;
(ii) resumption procedures;
(iii) a maintenance schedule for the plan;
(iv) awareness and education requirements;
(v) the responsibilities of the individuals;
(vi) recovery point objective (RPO) of fifteen minutes
(vii) recovery time objective (RTO) of 24 hours for essential CA operations which include certificate issuance, certificate revocation, and issuance of certificate revocation status; and
(viii) testing of recovery plans.

In order to mitigate the event of a disaster, Entrust has implemented the following:

(ix) secure on-site and off-site storage of backup HSMs containing copies of all CA Private Keys
(x) secure on-site and off-site storage of all requisite activation materials
(xi) regular synchronization of critical data to the disaster recovery site
(xii) regular incremental and daily backups of critical data within the primary site
(xiii) weekly backup of critical data to a secure off-site storage facility
(xiv) secure off-site storage of disaster recovery plan and disaster recovery procedures
(xv) environmental controls as described in §5.1
(xvi) high availability architecture for critical systems

Entrust has implemented a secure disaster recovery facility that is greater than 250 km from the primary secure CA facilities.

Entrust requires rigorous security controls to maintain the integrity of Entrust Certification Authorities. The Compromise of the Private Key used by an Entrust Certification Authority is viewed by Entrust as being very unlikely; however, Entrust has policies and procedures that will be employed in the event of such a Compromise. At a minimum, all Subscribers shall be informed as soon as practicable of such a Compromise and information shall be posted in the Entrust Repository.

4.9 CA Termination

In the event that an Entrust Certification Authority ceases operation, all Entrust Certificates issued by such Entrust Certification Authority shall be revoked and the CRL life-time will be set to a period that meets any Entrust obligations.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The hardware and software for an Entrust Certification Authority is located in a secure facility with physical security and access control procedures that meet or exceed industry standards. The CA equipment is located in a Security zone that is physically separated from Entrust's other systems so that only authorized CA personnel can access it.

5.1.2 Physical Access

The room containing the Entrust Authority software is designated a two (2) person zone, and controls are used to prevent a person from being in the room alone. Alarm systems are used to notify security personnel of any violation of the rules for access to an Entrust Certificate Authority.

5.1.3 Power and Air Conditioning

The Security zone is equipped with:

- Filtered, conditioned, power connected to an appropriately sized UPS and generator;
- Heating, ventilation, and air conditioning appropriate for a commercial data processing facility; and
- Emergency lighting.

The environmental controls conform to local standards and are appropriately secured to prevent unauthorized access and/or tampering with the equipment. Temperature control alarms and alerts are activated upon detection of threatening temperature conditions.

5.1.4 Water Exposures

No liquid, gas, exhaust, etc. pipes traverse the controlled space other than those directly required for the area's HVAC system and for the pre-action fire suppression system. Water pipes for the pre-action fire suppression system are only filled on the activation of multiple fire alarms.

5.1.5 Fire Prevention and Protection

The Entrust facility is fully wired for fire detection, alarm and suppression. Routine, frequent inspections of all systems are made to assure adequate operation.

5.1.6 Media Storage

All media is stored away from sources of heat and from obvious sources of water or other obvious hazards. Electromagnetic media (e.g. tapes) are stored away from obvious sources of strong magnetic fields. Archived material is stored in a room separate from the CA equipment until it is transferred to the archive storage facility.

5.1.7 Waste Disposal

Waste is removed or destroyed in accordance with industry best practice. Media used to store sensitive data is destroyed, such that the information is unrecoverable, prior to disposal.

5.1.8 Off-site Backup

As stipulated in §4.6.

5.2 Procedural Controls

An Entrust Certification Authority has a number of trusted roles for sensitive operations of the Entrust Certification Authority software. To gain access to the Entrust Authority software used in an Entrust Certification Authority, operational personnel must undergo background investigations. Entrust

Certification Authority operations related to adding administrative personnel or changing Certification Authority policy settings require more than one (1) person to perform the operation.

5.3 Personnel Controls

Operational personnel for an Entrust Certification Authority will not be assigned other responsibilities that conflict with their operational responsibilities for the Entrust Certification Authority. The privileges assigned to operational personnel for an Entrust Certification Authority will be limited to the minimum required to carry out their assigned duties.

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The signing Key Pair for an Entrust Certification Authority is created during the initial startup of the Entrust Master Control application and is protected by the master key for such Entrust Certification Authority.

When not generated by Entrust, the Applicant or Subscriber is required to generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Entrust Certificate or Applicant's Entrust Certificate Application.

Entrust Certification Authority Administrators
Keys Pairs for Entrust Certification Authority administrators must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 2 certification standards. The cryptographic modules are prepared using the software provided by the module vendor. The cryptographic modules are personalized for the administrator by giving the card an identity and a password known by the administrator. The Key Pair is generated by creating the administrator as a user in the Certification Authority and performing an enrollment process which is authenticated with the administrator's module password.

Entrust Client Certificates
In order to support key backup, Entrust may optionally provide a service to generate the Key Pair on behalf of the Applicant or Subscriber. The Key Pair is generated using a FIPS 140-2 Level 1 certified software toolkit. The prime number generator is in accordance with FIPS 186-2.

6.1.2 Private Key Delivery to Entity

Entrust Certificate Authorities do not generate the Key Pair on behalf of the Subscriber with the exception of Entrust Client Certificates.

Entrust Client Certificates
In the case where the Key Pair is generated on behalf of the Subscriber by the Entrust Certification Authority, the Private Key shall be delivered to the Subscriber in a cryptographically secure manner.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be included in an Entrust Certificate is delivered to Entrust Certification Authorities in a signed Certificate Signing Request (CSR) as part of the Entrust Certificate Application process. The signature on the CSR will be verified by the Entrust Certification Authority prior to issuing the Entrust Certificate.

6.1.4 CA Public Key Delivery to Users

The Public-Key Certificate for Entrust Certification Authorities are made available to Subscribers and Relying parties through inclusion in third party software as distributed by the applicable software manufacturers. The Public Key Certificate for cross certified issuing Certification Authorities is provided to the Subscriber with the Subscriber certificate.

Public Key Certificates for Entrust Certification Authorities are also available for download from the Repository.

6.1.5 Key Sizes

For Entrust Certification Authorities, the minimum key size shall be no less than 2048 bit RSA or shall be elliptic curve cryptography (ECC) NIST P-384 or P-521.

Entrust SSL Certificates
The minimum RSA key size is 2048 bits. The ECC keys supported are NIST P-256, P-384 and P-521.

Entrust Client Certificates
The minimum key size is RSA 2048 bits.

Entrust Code Signing Certificates
The minimum key size is RSA 2048 bits. As of January 1, 2021, the minimum key size is RSA 3072 bits. The ECC keys supported are NIST P-256, P-384 and P-521.
As of January 1, 2021, the minimum key size for new Entrust Certification Authority certificates which issue Entrust Code Signing Certificates is 3072 bit RSA and ECC NIST P-384 and P-521.

Entrust Document Signing Certificates
The minimum key size is RSA 2048 bits.

Entrust Time-Stamp Certificates
The minimum key size is RSA 2048 bits. As of January 1, 2021, the minimum key size is RSA 3072 bits. The ECC keys supported are NIST P-256, P-384 and P-521.

6.1.6 Public-Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

Certification Authority Key Pairs must be generated on a cryptographic module that meets or exceeds the requirements as defined in §6.8.

Root Certification Authority
Certificate issuance by the Root Certification Authority shall require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root Certification Authority to perform a certificate signing operation.

Root Certification Authority Private Keys must not be used to sign Certificates except in the following cases:

(i) Self-signed Certificates to represent the Root CA itself;
(ii) Certificates for Subordinate CAs and Cross Certificates;
(iii) Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates); and
(iv) Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA.

Entrust Document Signing Certificates
Subscriber Key Pairs must be generated in a manner that ensures that the Private Key is not known to or accessible by anybody other than the Subscriber or a Subscriber's authorized representative. Subscriber Key Pairs must be generated in a cryptographic module that prevents exportation or duplication and that meets or exceed the requirements as defined in §6.8.

Temporary Key Pairs and corresponding Entrust Document Signing Certificates may be generated by the Entrust Certification Authority for the limited purpose of testing. The test certificates must not contain actual identities and must be clearly marked for testing purposes only. These temporary test Key Pairs are exempt from the requirements in §6.8.

Entrust Time-Stamp Certificates
Subscriber Key Pairs must be generated in a manner that ensures that the Private Key is not known to or accessible by anybody other than the Subscriber or a Subscriber's authorized representative. Subscriber Key Pairs must be generated in a cryptographic module that prevents exportation or duplication and that meets or exceed the requirements as defined in §6.8.

6.1.9 Key Usage Purposes

Entrust Certificates issued by an Entrust Certification Authority contain the keyUsage and the extendkeyUsage Certificate extensions restricting the purpose for which an Entrust Certificate can be used as listed in Appendix A. Subscribers and Relying Parties shall only use Entrust Certificates in compliance with this Entrust CPS and applicable laws.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

Entrust Certification Authorities Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements as defined in §6.8. Private Keys on cryptographic modules are held in secure facilities under two-person control. RA Private Keys must be stored and protected on cryptographic modules that meet or exceed the requirements defined in §6.8.

Entrust Client Certificates
For cases where the Entrust Certification Authority has generated the Key Pair on behalf of the Subscriber, the Entrust Certification Authority shall use cryptographic modules which meet FIPS 140-2 Level 1.

Entrust Document Signing Certificates
Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Entrust Certificate. Subscribers must use cryptographic hardware modules that meet or exceed the requirements as defined in §6.8. Temporary key pairs generated by the Entrust Certification Authority for testing purposes pursuant to §6.1.1 are exempt from the requirements in §6.8.

6.2.2 Private Key Multi-Person Control

A minimum of two person control shall be established on any Entrust CA Private Key for all purposes including activation and backup, and may be implemented as a combination of technical and procedural controls. Persons involved in management and use of the Entrust CA Private Keys shall be designated as authorized by the CA for this purpose. The names of the parties used for two-person control shall be maintained on a controlled list.

6.2.3 Private Key Escrow

Entrust does not escrow the Entrust Certification Authorities' Private Keys.

6.2.4 Private Key Backup

Entrust CA Private Keys shall be backed up under the two-person control used to create the original version of the Private Keys. All copies of the Entrust CA Private Key shall be securely protected.

Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Entrust Certificate.

Entrust Client Certificates
For cases where the Entrust Certification Authority has generated the Key Pair on behalf of the Subscriber, the Entrust Certification Authority shall securely maintain a backup copy of the Private Key during the term of services.

6.2.5 Private Key Archival

Upon retirement of an Entrust CA, the Private Keys will be archived securely using hardware cryptographic modules that meet the requirements §6.8. The Key Pairs shall not be used unless the CA has been removed from retirement or the keys are required temporarily to validate historical data. Private Keys required for temporary purposes shall be removed from archive for a short period of time.

The archived Entrust CA Private Keys will be reviewed on an annual basis. After the minimum period of 5 years, the Entrust CA Private Keys may be destroyed according to the requirements in §6.2.10. The Entrust CA Private Keys must not be destroyed if they are still required for business or legal purposes.

Entrust Client Certificates
For cases where the Entrust Certification Authority has generated the Key Pair on behalf of the Subscriber, the Entrust Certification Authority may securely maintain an archive of the Subscriber Private Key in the secure long-term backups.

6.2.6 Private Key Entry into Cryptographic Module

Entrust CA Private Keys shall be generated by and secured in a cryptographic module. In the event that a Private Key is to be transported from one cryptographic module to another, the Private Key must be migrated using the secure methodology supported by the cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

Private Keys are stored on a cryptographic module are secured in accordance with the requirements specified in FIPS 140.

6.2.8 Method of Activating Private Keys

Entrust CA Private Keys shall be activated under two-person control using the methodology provided with the cryptographic module.

Subscriber Private Keys shall be activated by the Subscriber to meet the requirements of the security software used for their applications. Subscribers shall protect their Private Keys corresponding to the requirements in §2.1.3.

6.2.9 Private Key Deactivation Methods

Entrust CA Private Keys shall be deactivated when the CA is not required for active use. Deactivation of the Private Keys shall be done in accordance with the methodology provided with the cryptographic module.

Entrust Certification Authority Administrators
The administrator's identity is deactivated in the Entrust CA and the administrator's certificate is revoked.

6.2.10 Private Signature Key Destruction Method

Entrust CA Private Keys destruction will be two-person controlled and may be accomplished by executing a "zeroize" command or by destruction of the cryptographic module. Destruction of Entrust CA Private Keys must be authorized by the Entrust Policy Authority.

If the Entrust CA is removing a cryptographic module from service, then all Private Keys must be removed from the module. If the Entrust CA cryptographic module is intended to provide tamper-evident characteristics is removed from service, then the device will be destroyed.

Entrust Certification Authority Administrators
The administrator's private is destroyed by reinitializing the cryptographic module.

Entrust Client Certificates
For cases where the Entrust Certification Authority has generated the Key Pair on behalf of the Subscriber, Private Keys which have been archived will be destroyed in accordance with the backup destruction process.

6.3 Other Aspects of Key Pair Management

Entrust Certification Authority 2048-bit RSA Key Pairs may have a validity period expiring no later than 31 December 2030.

Entrust SSL Certificates
Entrust SSL Certificates contain a validity period of up to, but no more than, 39 months.

Entrust Client Certificates
Entrust Client Certificates contain a validity period of up to, but no more than, 39 months.

Entrust Code Signing Certificates
Entrust Code Signing Certificates contain a validity period of up to, but no more than, 39 months.

Entrust Document Signing Certificates
Entrust Document Signing Certificates contain a validity period of up to, but no more than, 39 months.

Entrust Time-Stamp Certificates
Entrust Time-Stamp Certificates contain a validity period of up to, but no more than 135 months.

6.4 Activation Data

No stipulation.

6.5 Computer Security Controls

The workstations on which the Entrust Certification Authorities operate are physically secured as described in §5.1. The operating systems on the workstations on which the Entrust Certification Authorities operate enforce identification and authentication of users. Access to Entrust Authority software databases and audit trails is restricted as described in this Entrust CPS. All operational personnel that are authorized to have access to the Entrust Certification Authorities are required to use hardware tokens in conjunction with a PIN to gain access to the physical room that contains the Entrust Authority software being used for such Entrust Certification Authorities.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

The Entrust Certification Authority makes use of Commercial Off The Shelf (COTS) products for the hardware, software, and network components. Systems developed by the Entrust Certification Authority are deployed in accordance with Entrust software lifecycle development standards.

6.6.2 Security Management Controls

The configuration of the Entrust Certification Authority system as well as any modifications and upgrades are documented and controlled. Methods of detecting unauthorized modifications to the CA equipment and configuration are in place to ensure the integrity of the security software, firmware, and hardware for correct operation. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system.

When first loaded, the CA software is verified as being that supplied from the vendor, with no modifications, and be the version intended for use.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Remote access to Entrust Certification Authority application via the Administration software interface is secured.

6.8 Cryptographic Module Engineering Controls

Certification Authority Key Pairs must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 3 certification standards.

Entrust Certification Authority Administrators

Key Pairs for Entrust Certification Authority administrators must be generated and protected on a cryptographic module that is compliant to at least FIPS 140-2 Level 2 certification standards.

Entrust Code Signing Certificates

Subscriber Key Pairs must be generated and protected in one of the following options:

(i) A Trusted Platform Module (TPM) that generates and secures a key pair and that can document the Subscriber's private key protection through a TPM key attestation

(ii) A hardware cryptographic module with a unit design form factor certified as conforming to at least FIPS 140 Level 2, Common Criteria EAL 4+, or equivalent.

(iii) Another type of hardware storage token with a unit design form factor of SD Card or USB token (not necessarily certified as conformant with FIPS 140 Level 2 or Common Criteria EAL 4+). The Subscriber MUST also warrant that it will keep the token physically separate from the device that hosts the code signing function until a signing session is begun.

Entrust Document Signing Certificates

Subscriber Key Pairs must be generated and protected in a cryptographic module that meets or exceed FIPS 140-2 Level 2 certification standards.

Entrust Time-Stamp Certificates

Subscriber Key Pairs must be generated and protected in a cryptographic module that meets or exceed FIPS 140-2 Level 3 certification standards.

6.9 Time-Stamping

Entrust provides a Time-Stamp Authority (TSA) service for use with specific Entrust products such as Entrust Code Signing and Document Signing Certificates. The TSA authority supports RFC 3161 "Internet X.509 Public Key Infrastructure Time-Stamp Protocol" and Microsoft Authenticode™ time-stamp requests.

Details of any acceptable use policy or limitations are included in the Subscription Agreement.

7 Certificate and CRL Profiles

The profile for the Entrust Certificates and Certificate Revocation List (CRL) issued by an Entrust Certification Authority conform to the specifications contained in the IETF RFC 5280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

Entrust Certificates shall have a serial number greater than zero (0) that contains at least 64 unpredictable bits.

7.1 Certificate Profile

Entrust Certification Authorities issue certificates in accordance with the X.509 version 3. Certificate profiles for Entrust Root CA certificate, Subordinate CA certificates, and end entity certificates are described in Appendix A and the sections below.

7.1.1 Version Number(s)

All certificates issued by Entrust Certification Authorities are X.509 version 3 certificates.

7.1.2 Certificate Extensions

Certificate extensions are as stipulated in IETF RFC 5280. See Appendix A.

7.1.3 Algorithm Object Identifiers

Algorithm object identifiers are as specified in IETF RFC 3279 Algorithms and Identifiers for the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile. See Appendix A.

7.1.4 Name Forms

Name forms are as stipulated in §3.1.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Certificate policy object identifiers (OIDs) are listed in §1.2 and in the Certificate Profile attached as Appendix A.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

Entrust includes policy qualifiers in all end entity certificates as stipulated in Appendix A.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificate policies extension is marked Not Critical

7.2 CRL Profile

The following fields of the X.509 version 2 CRL format are used by the Entrust Certification Authorities:

- version: set to v2
- signature: identifier of the algorithm used to sign the CRL
- issuer: the full Distinguished Name of the Certification Authority issuing the CRL
- this update: time of CRL issuance
- next update: time of next expected CRL update
- revoked certificates: list of revoked Certificate information

7.3 OCSP Profile

The profile for the Entrust SSL Online Certificate Status Protocol (OCSP) messages issued by an Entrust Certification Authority conform to the specifications contained in the IETF RFC 2560 Internet X.509 PKI Online Certificate Status Protocol (OCSP) Profile.

7.4 Certificate Transparency

Entrust SSL Certificates

Entrust SSL Certificates may include two or more signed certificate timestamps (SCT) from Google approved independent certificate transparency logs. Information on certificate transparency may be found in IETF RFC 6962.

8 Specification Administration

8.1 Specification Change Procedures

Entrust may, in its discretion, modify the Entrust CPS and the terms and conditions contained herein from time to time. Entrust shall modify the CPS to stay concurrent with the latest version of the Baseline Requirements.

Modifications to the Entrust CPS shall be published in the Entrust Repository and shall become effective fifteen (15) days after publication in the Entrust Repository unless Entrust withdraws such modified Entrust CPS prior to such effective date. In the event that Entrust makes a significant modification to Entrust CPS, the version number of the Entrust CPS shall be updated accordingly. Unless a Subscriber ceases to use, removes, and requests revocation of such Subscriber's Entrust Certificate(s) prior to the date on which an updated version of the Entrust CPS becomes effective, such Subscriber shall be deemed to have consented to the terms and conditions of such updated version of the Entrust CPS and shall be bound by the terms and conditions of such updated version of the Entrust CPS.

8.2 Publication and Notification Policies

Prior to major changes to this Entrust CPS, notification of the upcoming changes will be posted in the Entrust Repository.

8.3 CPS Approval Procedures

This Entrust CPS and any subsequent changes shall be approved by the Entrust Policy Authority.

9 Acronyms

ASV	Application Software Vendor
CA	Certification Authority
CAA	Certification Authority Authorization
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DN	Distinguished Name
DNS	Domain Name Server
DSA	Digital Signature Algorithm
ECC	Elliptic Curve Cryptography
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MAC	Message Authentication Code
OA	Operational Authority
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PA	Policy Authority
PIN	Personal Identification Number
PKI	Public-Key Infrastructure
RA	Registration Authority
RDN	Relative Distinguished Name
RFC	Request for Comment
SEP	Secure Exchange Protocol
SSL	Secure Sockets Layer
TSA	Time-Stamp Authority
URL	Universal Resource Locator

10 Definitions

Affiliate: means collectively, Entrust Datacard Corporation and any 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. In this context, a party "controls" a corporation or another entity if it directly or indirectly owns or controls fifty percent (50%) or more of the voting rights for the board of directors or other mechanism of control or, in the case of a non-corporate entity, an equivalent interest.

Applicant: means a person, entity, or organization applying for an Entrust Certificate, but which has not yet been issued an Entrust Certificate, or a person, entity, or organization that currently has an Entrust Certificate or Entrust Certificates and that is applying for renewal of such Entrust Certificate or Entrust Certificates or for an additional Entrust Certificate or Entrust Certificates.

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.

ASV: see Application Software Vendor.

Baseline Requirements: CA/Browser Forum Guidelines Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org. The Baseline Requirements describe certain minimum requirements that a Certification Authority (CA) must meet in order to issue SSL Certificates. In the event of any inconsistency between this CPS and the Baseline Requirements, the Baseline Requirements take precedence over this CPS.

Business Day: means any day, other than a Saturday, Sunday, statutory or civic holiday in the City of Ottawa, Ontario.

Certificate: means a digital document that at a minimum: (a) identifies the Certification Authority issuing it, (b) names or otherwise identifies a Subject, (c) contains a Public Key of a Key Pair, (d) identifies its operational period, and (e) contains a serial number and is digitally signed by a Certification Authority.

Certificate Approver: means an employee or agent authorized to approve a request for an Entrust Certificate for an organization.

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 Operational Period of such Certificate.

Certificate Requester: means an employee or agent authorized to request an Entrust Certificate for an organization.

Certificate Revocation List: means a time-stamped list of the serial numbers of revoked Certificates that has been digitally signed by a Certification Authority.

Certification Authority: means an entity or organization that (i) creates and digitally signs Certificates that contain among other things a Subject's Public Key and other information that is intended to identify the Subject, (ii) makes Certificates available to facilitate communication with the Subject identified in the Certificate, and (iii) creates and digitally signs Certificate Revocation Lists containing information about Certificates that have been revoked and which should no longer be used or relied upon.

Certification Practice Statement: means a statement of the practices that a Certification Authority uses in issuing, managing, revoking, renewing, and providing access to Certificates, and the terms and conditions under which the Certification Authority makes such services available.

Co-marketers: means any person, entity, or organization that has been granted by Entrust or a Registration Authority operating under an Entrust Certification Authority the right to promote Entrust Certificates.

Compromise: means a suspected or actual loss, disclosure, or loss of control over sensitive information or data.

Contract Signer: means an employee or agent authorized to sign the subscription agreement on behalf of the organization.

CPS: see Certification Practice Statement.

CRL: see Certificate Revocation List.

Cross Certificate(s): shall mean a Certificate(s) that (i) includes the Public Key of a Public-Private Key Pair generated by an Entrust Certification Authority; and (ii) includes the digital signature of an Entrust Root Certification Authority.

Entrust: means Entrust Limited.

Entrust.net: means Entrust Limited.

Entrust Operational Authority: means those personnel who work for or on behalf of Entrust and who are responsible for the operation of the Entrust Certification Authorities.

Entrust Policy Authority: means those personnel who work for or on behalf of Entrust and who are responsible for determining the policies and procedures that govern the operation of the Entrust Certification Authorities.

Entrust Repository: means a collection of databases and web sites that contain information about Entrust Certificates and services provided by Entrust in respect to Entrust Certificates, including among other things, the types of Entrust Certificates issued by the Entrust Certification Authorities, the services provided by Entrust in respect to Entrust Certificates, the fees charged by Entrust for Entrust Certificates and for the services provided by Entrust in respect to Entrust Certificates, Certificate Revocation Lists, the Entrust Certification Practice Statement, and other information and agreements that are intended to govern the use of Entrust Certificates.

Entrust Certificate: A Certificate issued by an Entrust Certification Authority.

Entrust Certification Authority: means a Certification Authority operated by or on behalf of Entrust for the purpose of issuing, managing, revoking, renewing, and providing access to Entrust Certificates.

Entrust Certification Practice Statement: means this document.

Entrust CPS: See Entrust Certification Practice Statement.

Entrust Client Certificate: means a Certificate issued by an Entrust Certificate Authority for use by individuals to digitally sign and encrypt electronic messages via an S/MIME compliant application.

Entrust Code Signing Certificate: means a Certificate issued by an Entrust Certification Authority for use by content and software developers and publishers to digitally sign executables and other content.

Entrust Document Signing Certificate: means a Certificate issued by an Entrust Certification Authority for use by individuals or systems to digitally sign documents.

Entrust Group: means collectively, Entrust, Affiliates, independent third-party Registration Authorities, Resellers, Co-Marketers, distributors, subcontractors, agents, suppliers and any employees and directors of the foregoing.

Entrust SSL Certificate: means an SSL Certificate issued by an Entrust Certification Authority for use on secure servers.

Entrust Time-Stamp Certificate: means a Certificate issued by an Entrust Certification Authority for use by a time-stamp authority to digitally sign time-stamp tokens.

Entrust Certificate Application: means the form and application information requested by a Registration Authority operating under an Entrust Certification Authority and submitted by an Applicant when applying for the issuance of an Entrust Certificate.

FIPS: means the Federal Information Processing Standards. These are U.S. Federal standards that prescribe specific performance requirements, practices, formats, communication protocols, and other requirements for hardware, software, data, and telecommunications operation.

IETF: means the Internet Engineering Task Force. The Internet Engineering Task Force is an international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the efficient operation of the Internet.

Key Pair: means two mathematically related cryptographic keys, having the properties that (i) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is believed to be computationally infeasible to discover the other key.

Minimum Requirements for Code Signing: means Minimum Requirements for Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates published at https://aka.ms/csbr. The Minimum Requirements for Code Signing describe certain minimum requirements that a Certification Authority (CA) must meet in order to issue Code Signing Certificates.

Object Identifier: means a specially-formatted sequence of numbers that is registered in accordance with internationally-recognized procedures for object identifier registration.

OID: see Object Identifier.

Operational Period: means, with respect to a Certificate, the period of its validity. The Operational Period would typically begin on the date the Certificate is issued (or such later date as specified in the Certificate), and ends on the date and time it expires as noted in the Certificate or earlier if the Certificate is Revoked.

PKIX: means an IETF Working Group developing technical specifications for PKI components based on X.509 Version 3 Certificates.

Private Key: means the key of a Key Pair used to decrypt an encrypted message. This key must be kept secret.

Public Key: means the key of a Key Pair used to encrypt a message. The Public Key can be made freely available to anyone who may want to send encrypted messages to the holder of the Private Key of the Key Pair. The Public Key is usually made publicly available in a Certificate issued by a Certification Authority and is often obtained by accessing a repository or database. A Public Key is used to encrypt a message that can only be decrypted by the holder of the corresponding Private Key.

RA: see Registration Authority.

Registration Authority: means an entity that performs two functions: (1) the receipt of information from a Subject to be named in an Entrust Certificate, and (2) the performance of limited verification of information provided by the Subject following the procedures prescribed by the Entrust Certification Authorities. In the event that the information provided by a Subject satisfies the criteria defined by the Entrust Certification Authorities, a Registration Authority may send a request to an Entrust Certification Authority requesting that the Entrust Certification Authority generate, digitally sign, and issue an Entrust Certificate containing the information verified by the Registration Authority.

Relying Party: means a person, entity, or organization that relies on or uses an Entrust Certificate and/or any other information provided in a Repository under an Entrust Certification Authority to obtain and confirm the Public Key and identity of a Subscriber. For avoidance of doubt, an ASV is not a "Relying Party" when software distributed by such ASV merely displays information regarding a certificate.

Relying Party Agreement: means the agreement between a Relying Party and Entrust or between a Relying Party and an independent third-party Registration Authority or Reseller under an Entrust Certification Authority in respect to the provision and use of certain information and services in respect to Entrust Certificates.

Repository: means a collection of databases and web sites that contain information about Certificates issued by a Certification Authority including among other things, the types of Certificates and services provided by the Certification Authority, fees for the Certificates and services provided by the Certification

Authority, Certificate Revocation Lists, descriptions of the practices and procedures of the Certification Authority, and other information and agreements that are intended to govern the use of Certificates issued by the Certification Authority.

Resellers: means any person, entity, or organization that has been granted by Entrust or a Registration Authority operating under an Entrust Certification Authority the right to license the right to use Entrust Certificates.

Revoke or Revocation: means, with respect to a Certificate, to prematurely end the Operational Period of that Certificate from a specified time forward.

Subordinate CA Certificate: shall mean a Certificate that (i) includes the Public Key of a Public-Private Key Pair generated by a Certification Authority; and (ii) includes the digital signature of an Entrust Root Certification Authority.

Subject: means a person, entity, or organization whose Public Key is contained in a Certificate.

Subscriber: means a person, entity, or organization that has applied for and has been issued an Entrust Certificate.

Subscription Agreement: means the agreement between a Subscriber and Entrust (or an Affiliate of Entrust) or between a Subscriber and an independent third-party Registration Authority or Reseller under an Entrust Certification Authority in respect to the issuance, management, and provision of access to an Entrust Certificate and the provision of other services in respect to such Entrust Certificate.

Third Party Subordinate CA: means a Subordinate CA Certificate issued to a CA owned by a third party.

Appendix A – Certificate Profiles

Root Certificate: Entrust.net Certification Authority (2048)

Field		**Value**
Attributes		
Version		V3
Serial Number		38 63 b9 66
Signature Algorithm		sha-1 WithRSAEncryption {1.2.840.113549.1.1.5}
Issuer DN		CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net
Validity Period		Valid from: December 24, 1999 Valid to: December 24, 2019
Subject DN		CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net
Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	KeyID=55 e4 81 d1 11 80 be d8 89 b9 08 a3 31 f9 a1 24 09 16 b9 70
Subject Key Identifier	No	55 e4 81 d1 11 80 be d8 89 b9 08 a3 31 f9 a1 24 09 16 b9 70
Thumbprint (SHA1)		80 1d 62 d0 7b 44 9d 5c 5c 03 5c 98 ea 61 fa 44 3c 2a 58 fe

Root Certificate: Entrust.net Certification Authority (2048) - (Updated)

Field		**Value**
Attributes		
Version		V3
Serial Number		38 63 de f8
Signature Algorithm		sha-1 WithRSAEncryption {1.2.840.113549.1.1.5}
Issuer DN		CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net
Validity Period		Valid from: December 24, 1999 Valid to: July 24, 2029
Subject DN		CN = Entrust.net Certification Authority (2048) OU = (c) 1999 Entrust.net Limited OU = www.entrust.net/CPS_2048 incorp. by ref. (limits liab.) O = Entrust.net
Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier		Not present
Subject Key Identifier	No	55 e4 81 d1 11 80 be d8 89 b9 08 a3 31 f9 a1 24 09 16 b9 70
Key Usage	Yes	Certificate Signing, CRL Signing
Certificate Policies		Not present
Basic Constraints		Subject Type=CA Path Length Constraint=None
CRL Distribution Points		Not present
Thumbprint (SHA1)		50 30 06 09 1d 97 d4 f5 ae 39 f7 cb e7 92 7d 7d 65 2d 34 31

Root Certificate: Entrust Root Certification Authority – G2

Field		**Value**
Attributes		
Version		V3
Serial Number		4a 53 8c 28
Signature Algorithm		sha-256 WithRSAEncryption {1.2.840.113549.1.1.5}
Issuer DN		CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US
Validity Period		Valid from: July 7, 2009 Valid to: December 7, 2030
Subject DN		CN = Entrust Root Certification Authority - G2 OU = (c) 2009 Entrust, Inc. - for authorized use only OU = See www.entrust.net/legal-terms O = Entrust, Inc. C = US
Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier		Not present
Subject Key Identifier	No	6a 72 26 7a d0 1e ef 7d e7 3b 69 51 d4 6c 8d 9f 90 12 66 ab
Key Usage	Yes	Certificate Signing, CRL Signing
Basic Constraints	Yes	Subject Type=CA Path Length Constraint=None
CRL Distribution Points		Not present
Thumbprint (SHA1)		8c f4 27 fd 79 0c 3a d1 66 06 8d e8 1e 57 ef bb 93 22 72 d4

Subordinate CA Certificate

Field		Value
Attributes		
Version		V3
Serial Number		Unique number to PKI domain
Signature Algorithm		sha-1 or sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		No later than 2030 notBefore and notAfter are specified
Subject DN		Unique X.500 CA DN
Subject Public Key Info		2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the Root CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Key Usage	Yes	Certificate Signing, CRL Signing
Extended Key Usage	No	As applicable from the following: None present Server Authentication (1.3.6.1.5.5.7.3.1) Client Authentication (1.3.6.1.5.5.7.3.2) Code Signing (1.3.6.1.5.5.7.3.3) Secure Email (1.3.6.1.5.5.7.3.4) Time Stamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	No	Policy Identifier = All Issuance Policies uri: set as applicable
Basic Constraints	Yes	Subject Type = CA Path Length Constraint = value set as required
Authority Information Access (optional)	No	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation=http://ocsp.entrust.net
CRL Distribution Points	No	http://crl.entrust.net/server1.crl or http://crl.entrust.net/2048ca.crl

SSL End Entity Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		No greater than 39 months notBefore and notAfter are specified
Subject DN		CN = <DNS name of secure server> OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048-bit RSA key modulus or EC Curve NIST P-256, P-384 or P-521
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Subject Alternative Name	No	DNS name(s) of secure server.
Signed Certificate Timestamps	No	1.3.6.1.4.1.11129.2.4.2 MAY include two or more signed certificate timestamps (Certificate Transparency proofs) from approved CT Logs.
Key Usage	Yes	RSA keys - Digital Signature, Key Encipherment ECC keys – Digital Signature
Extended Key Usage	No	Server Authentication (1.3.6.1.5.5.7.3.1) and/or Client Authentication (1.3.6.1.5.5.7.3.2)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier=**1.2.840.113533.7.75.2** or **2.16.840.1.114028.10.1.5** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=**2.23.140.1.2.2**
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None
Authority Information Access (optional)	No	Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation: http://ocsp.entrust.net Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation: http://aia.entrust.net/2048-l1c.cer or http://aia.entrust.net/l1k-chain256.cer
CRL Distribution Points	No	http://crl.entrust.net/level1c.crl or http://crl.entrust.net/level1k.crl

Code Signing End Entity Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-1 or sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		No greater than 39 months notBefore and notAfter are specified
Subject DN		CN = < full legal name of subscriber > OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Key Usage	Yes	Digital Signature
Extended Key Usage	No	Code Signing (1.3.6.1.5.5.7.3.3) Kernel Mode (1.3.6.1.4.1.311.61.1.1) (optional)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= **2.16.840.1.114028.10.1.3** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa [2]Certificate Policy: Policy Identifier=**2.23.140.1.4.1**
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None
Authority Information Access (optional)		Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation: http://ocsp.entrust.net Access Method = Certification Authority Issuer (1.3.6.1.5.5.7.48.2) accessLocation: http://aia.entrust.net/2048-l1d.cer or http://aia.entrust.net/2048-l1dsha2.cer or http://aia.entrust.net/ovcs1-chain256.cer
CRL Distribution Points	No	http://crl.entrust.net/level1d.crl or http://crl.entrust.net/ovcs1.crl

Client Class 1 End Entity Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-1 or sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		Not greater than 39 months notBefore and notAfter are specified
Subject DN		E = <RFC822 email address> CN = <RFC822 email address> OU = <Persona Not Validated> OU = <Entrust Class 1 Identity Certification Service>
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Subject Alternative Name		<RFC822 email address>
Key Usage	Yes	Digital Signature, Key Encipherment
Extended Key Usage	No	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= **2.16.840.1.114028.10.1.4.1** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa
Basic Constraints	No	Subject Type = End Entity, Path Length Constraint = None
Authority Information Access		1. Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net 2. Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.entrust.net/2048class1.cer or http://aia.entrust.net/2048class1sha2.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/class1ca.crl

Client Class 2 End Entity Certificate

Field		Value
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-1 or sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		Not greater than 39 months notBefore and notAfter are specified
Subject DN		E = <RFC822 email address> CN = < individual name, organization name or role name > OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber organization> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Subject Alternative Name		<RFC822 email address>
Key Usage	Yes	Digital Signature Key Encipherment Data Encipherment (optional)
Extended Key Usage	No	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= **2.16.840.1.114028.10.1.4.2** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa
Basic Constraints	No	Subject Type = End Entity, Path Length Constraint = None
Authority Information Access		1. Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net 2. Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://aia.entrust.net/2048class2.cer or http://aia.entrust.net/2048class2sha2.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/class2ca.crl

Document Signing End Entity Certificate

Field		Value
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		Not greater than 39 months notBefore and notAfter are specified
Subject DN		E = <RFC822 email address>(optional) CN = < individual name, organization name or role name > OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber organization> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Subject Alternative Name		<RFC822 email address> (optional)
Key Usage	Yes	Digital Signature Key Encipherment Non-repudiation
Extended Key Usage	No	Document Signing (1.3.6.1.4.1.311.10.3.12) Document Signing (2.16.840.1.114027.40.11)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= **2.16.840.1.114028.10.1.6** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None
Authority Information Access (optional)		1. Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ocsp.entrust.net 2. Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL= http://aia.entrust.net/class3-2048.cer
CRL Distribution Points	No	uri: http://crl.entrust.net/class3-sha2.crl
Archive Rev Info	No	30 03 02 01 01
Time-stamp (1.2.840.113583.1.1.9.1)	No	URI = http://timestamp.entrust.net/TSS/RFC3161sha2TS Authentication = Not Required

Time-Stamp End Entity Certificate

Field		**Value**
Attributes		
Version		V3
Serial Number		Unique number to PKI domain with 64 bits entropy
Issuer Signature Algorithm		sha-1 or sha-256
Issuer DN		Unique X.500 CA DN
Validity Period		Not greater than 135 months notBefore and notAfter are specified
Subject DN		E = <RFC822 email address> (optional) CN = <name associated with TSA> (optional) OU = <organization unit of subscriber> (optional) O = <full legal name of subscriber organization> L = <locality of subscriber> (optional) S = <state or province of subscriber> (if applicable) C = <country of subscriber>
Subject Public Key Info		Minimum 2048-bit RSA key modulus rsaEncryption {1.2.840.113549.1.1.1}
Extension	**Critical**	
Authority Key Identifier	No	Contains 20 byte SHA-1 hash of the CA Public Key
Subject Key Identifier	No	Contains 20 byte SHA-1 hash of the subjectPublicKey in this certificate
Key Usage	Yes	Digital Signature
Extended Key Usage	Yes	Time Stamping (1.3.6.1.5.5.7.3.8)
Certificate Policies	No	[1]Certificate Policy: Policy Identifier= **2.16.840.1.114028.10.1.7** [1,1]Policy Qualifier Info: Policy Qualifier Id=CPS Qualifier: http://www.entrust.net/rpa
Basic Constraints	No	Subject Type = End Entity Path Length Constraint = None
Authority Information Access (optional)		Access Method = On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) accessLocation: http://ocsp.entrust.net
CRL Distribution Points	No	uri: http://crl.entrust.net/ts1ca.crl

Appendix B – Subordinate CA Certificates

Entrust issues subordinate CA certificates to Entrust and third party operated CAs ("Third Party Subordinate CAs").

Entrust Subordinate CAs

Entrust operated subordinate CAs are managed in accordance with this CPS or are operated in accordance with their own CP and/or CPS which meets the minimum requirements of this CPS.

Third Party Subordinate CAs

Registration

Entrust specifies requirements to Third Party Subordinate CAs through written agreement. The Third Party Subordinate CAs must make use of a CP and/or CPS which meets the minimum requirements of this CPS. The generation of the CA key pair for the Third Party Subordinate CAs is to be witnessed by a third party security auditor.

A request for a subordinate certificate is started by the Third Party Subordinate CAs submitting a CSR. The CSR is authenticated by contacting the authorization contact for the Third Party Subordinate CAs.

Certificate Renewal

Third party CA certificates may be renewed through mutual agreement. The CA certificate may be renewed using the original CSR which was submitted for the initial registration. If the renewal is performed with a new CSR, then the CSR is authenticated by contacting the authorization contact of the Third Party Subordinate CAs.

Certificate Rekey

Third party CA certificates are rekeyed using a new CSR. The new CSR is authenticated by the authorization contact of the Third Party Subordinate CAs.

Certificate Issuance

The third party CA certificate is issued in accordance with the Subordinate CA Certificate profile defined in Appendix A.

Certificate Distribution

The third party CA certificate may be distributed in accordance with license set out in the agreement.

Certificate Revocation

Entrust confirms third party CA certificate revocation requests by contacting the authorization contact of the Third Party Subordinate CAs.

In addition to any other basis giving rise to a right to revoke a CA Certificate, Entrust may also revoke any CA certificate in accordance with the agreement between Entrust and the Subordinate Third Party CA.

The revocation status will be provided by CRL and/or OCSP.

Certification Authority Assessment

Third Party Subordinate CAs are assessed to meet the requirements of the CP and/or CPS on an annual basis using one of the audit criteria specified in the Baseline Requirements.

