ENTRUST CERTIFICATE SERVICES

Certification Practice Statement for Adobe CDS

Version: 1.4
December 1, 2013

Revision History

Issue	Date	Changes in this Revision
1.0	September 16, 2008	First version.
1.1	October 24, 2008	Entrust Legal
1.2	November 14, 2008	Adobe review
1.3	February 28, 2011	Update disaster recovery requirements and other minor revisions having no material impact.
1.4	December 1, 2013	Update for inclusion of data controls for certificate renewal, CRL issuance, time synchronization, and support for smartcards.

TABLE OF CONTENTS

1. Introduction

1.1 Overview

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 and digital signatures.

Certified Document Services (CDS) is a new platform offering first available in the Acrobat® 6.0 product family available from Adobe Systems Incorporated ("Adobe") which makes use of digital signature technology. CDS provides recipients with an improved assurance that certified PDF documents are authentic – i.e., that they did originate from their stated author and the portion of the document signed by the author has not been modified since authoring. Adobe and Entrust have partnered to enable Entrust to issue digital certificates for use within the CDS platform ("Entrust Certificate"). This Entrust Certification Practice Statement for Adobe CDS ("CPS") describes the practices and procedures that Entrust follows in issuing Entrust Certificates.

This CPS is incorporated by reference into all Entrust Certificate issued by Entrust, and is also incorporated by reference into the Subscriber Agreement pursuant to which Entrust licenses Certificates to Subscribers for use within the CDS platform.

1.2 Identification

This document is called the Entrust Certificate Services Certification Practice Statement for Adobe CDS ("CPS"). This CPS defines the practices followed by the Entrust Certification Authority for CDS ("Entrust CA") in issuing Entrust Certificates in accordance with the Adobe CDS Certificate Policy available at http://www.adobe.com/misc/pki/root_cp.html (or a successor website thereto) ("Adobe CP"). Each Entrust Certificate issued by Entrust for use within the CDS platform contains the following Object Identifiers (OID) defined in the Adobe CP.

- The Attribute Object Identifier (OID) for this Policy is: **1.2.840.113583.1.2.1**
- The extended key usage OID for the CDS PKI is: **1.2.840.113583.1.1.5**

1.3 Community and Application

The community for this CPS includes Entrust acting as a CDS Subordinate CA (as defined within the context of the Adobe CP), RAs, and Subscribers whose certificates chain to the Adobe Root CA embedded in Acrobat® by Adobe, along with all Relying Parties who rely on such certificates.

Certificates issued by Entrust for use within the CDS platform:

- will have the certificate policy extension populated with the OID identified in §1.2, and
- may only be used by Subscribers for signing Adobe Acrobat documents.

1.3.1 Certification Authorities

Entrust is acting as a Certification Authority (CA) to create and issue CDS certificates to Subscribers under the Adobe CP.

1.3.2 Registration Authorities

Entrust may appoint Registration Authorities (RAs) to manage the certificate lifecycle for the Entrust CA, and otherwise delegate its obligations to subcontractors provided that Entrust remains responsible for the performance of such subcontractors. Any such RAs are responsible for issuing and revoking certificates in accordance with its contract with Entrust and this CPS, as well as the Adobe CP.

1.3.3 End Entities

End Entities are Subscribers and Relying Parties. A Subscriber is any authorized individual, hardware device or organization that has an Entrust Certificate issued to them and uses that certificate to sign a CDS document.

Relying Parties are recipients of CDS documents who wish to verify the Subscriber's signature.

1.3.4 Applicability

Entrust Certificates are to be used only for digitally signing and verifying Adobe Acrobat documents. Entrust Certificates conform to the requirements of the ITU-T X.509 v3 standard.

1.4 Contact Details

1.4.1 Specification Administration Organization

This CPS is administered by the Entrust Policy Authority, which consists of selected members of Entrust's management team.

1.4.2 Contact Person

The contact information for questions about Entrust Certificates is:

Entrust Limited
1000 Innovation Drive
Ottawa, Ontario
Canada K2K 3E7
Attn: Entrust CDS Policy Authority

Tel: 1-877-368-7483
Fax: 1-877-839-3538

Email: certserv.support@Entrust.com

2. General Provisions

2.1 Obligations

2.1.1 Certification Authority Obligations

Entrust warrants to all Relying Parties placing reasonable reliance on an Entrust Certificate that:

(i) Entrust took reasonable steps (no less than the procedures set forth in §3.1.8 and §3.1.9 of the Adobe CP) to verify the information contained in the Entrust Certificate is accurate,
(ii) information in the Entrust Certificate accurately reflects the information provided to Entrust by the Subscriber in all material respects,
(iii) Each Subscriber has accepted the Entrust CDS Certificate according to the provisions of this CPS and the Adobe CP, and
(iv) Entrust has complied in all material respects with the Adobe CP and this CPS.

2.1.2 Registration Authority Obligations

Entrust may delegate specific registration activities to one or more CDS RAs, provided that Entrust remains responsible for the services provided by its CDS RAs and the CDS CA warrants that the activities of its CDS RAs will be conducted in accordance with this policy. A CDS RA shall perform all delegated registration functions in accordance with its agreement with Entrust, the requirements of the Adobe CP, and this CPS.

2.1.3 Subscriber Obligations

A Subscriber shall:

(i) accurately represent itself in all communications with Entrust and any RAs;
(ii) at all times, protect the private key associated with the public key in any Entrust Certificates;
(iii) notify, in a timely manner, Entrust of any suspicion that its private key is compromised or is reasonably believed to have been compromised. Such notification shall be to the Entrust Policy Authority as identified above; and
(iv) abide by all the terms, conditions, and restrictions in this CPS, the Adobe CP, and in the applicable Subscriber Agreement.

Entrust and Adobe reserve the right to revoke the Certificate of any Subscriber who violates the obligations specified in this CPS, the Adobe CP, and the applicable Subscriber Agreement.

Subscribers may either apply for Entrust Certificates directly, or an organization acting on behalf of a Subscriber or group of Subscribers may apply for Entrust Certificate(s).

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 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 Applicant is an Individual

When the applicant is an individual Subscriber applying for a certificate in the name of that individual or in the name of the role of that individual within an organization, the Subscriber will:

(i) generate a public key pair using a trustworthy system and take all reasonable precautions to prevent any loss, disclosure, or unauthorized use of the private key;
(ii) ensure all information and representations made by the Subscriber that are included in the certificate application are true;
(iii) upon receipt of an Entrust Certificate, acknowledge that the information identifying the Subscriber in the certificate is true and accurate, or notify Entrust immediately upon any inaccuracies in that information;
(iv) use the certificate exclusively for CDS purposes, consistent with this CPS, the Adobe CP, the Subscriber Agreement and all applicable laws;
(v) immediately send a written request to the Entrust CDS Policy Authority requesting certificate revocation upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key; and
(vi) immediately cease to use the Entrust Certificate upon (i) expiration or notification of revocation of such Entrust Certificate, or (ii) any suspected or actual Compromise of the Private Key corresponding to the Public Key in such Entrust Certificate, and destroy the Private Key corresponding to the Public Key contained in the Entrust Certificate in accordance with this CPS.

2.1.3.2 Applicant is an Organization Acquiring a Certificate on Behalf of an Individual Subscriber

When the applicant is an organization acquiring and managing an Entrust Certificate on behalf of an individual Subscriber (in the name of that individual or in the name of the role of that individual within the organization), the applicant organization is required to:

(i) maintain processes that assure that the private key can be used only with the knowledge and explicit action of the Subscriber;
(ii) maintain information that permits a determination of who signed a particular document;
(iii) ensure that the Entrust Certificate subject has received security training appropriate for the purposes for which the certificate is issued;
(iv) immediately send a written request to the Entrust CDS Policy Authority requesting certificate revocation upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;
(v) ensure that the Subscriber named in the certificate or responsible for the use of the private key corresponding to the public key in the certificate agrees to comply with this CPS, the Adobe CP, the Subscriber Agreement, and all applicable laws.

2.1.3.3 Applicant is an Organization Acquiring and Managing a Certificate on behalf of the Organization (i.e., an organizational certificate)

When the applicant is an organization acquiring and managing a certificate on behalf of the organization (i.e., an organizational certificate), the applicant organization will:

(i) maintain processes, including, without limitation, changing of activation data, that assure that each private key can be used only with the knowledge and explicit action of only one human being within the organization (the certificate custodian);
(ii) maintain information that permits a determination of who signed a particular document;
(iii) ensure that the certificate custodian has received security training appropriate for the purposes for which the certificate is issued;
(iv) prevent sharing of organizational certificates amongst members of the organization;

(v) acknowledge that the information identifying the organization in the certificate is true and accurate, or notify Entrust immediately upon any inaccuracies in that information;
(vi) immediately send a written request to the Entrust CDS Policy Authority requesting certificate revocation upon any actual or suspected loss, disclosure, or other compromise of the Subscriber's private key;
(vii) ensure that the certificate custodian agrees to also be bound by the Subscriber Agreement, this CPS, the Adobe CP and all applicable laws.

2.1.3.4 Subscriber and Applicant Representations and Warranties

Subscribers and Applicants represent and warrant to Entrust, Adobe and all third parties who rely or use the Entrust Certificate issued to such Subscriber, that:

(i) all information provided to Entrust or to any RAs, both in the Certificate Request and as otherwise requested by Entrust in connection with the issuance of the Certificate(s) to be supplied by Entrust, is accurate and complete and does not contain any errors, omissions, or misrepresentations;
(ii) the Private Key corresponding to the Public Key submitted to Entrust in connection with an Entrust Certificate Application was created using sound cryptographic techniques and 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;
(iii) any information provided to Entrust or to any RAs 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;
(iv) the Certificate(s) shall not be installed or used until it has reviewed and verified the accuracy of the data in each Certificate;
(v) use of the Certificate shall be exclusively for signing Acrobat documents;
(vi) Entrust shall be immediately notified if any information included in the Entrust Certificate Application changes or if a change in circumstances would make the information in the Entrust Certificate Application misleading or inaccurate;
(vii) all use of the Entrust Certificate and its associated private key shall cease immediately, and the Subscriber shall notify Entrust and promptly request the revocation of the Entrust Certificate, if (1) any information included in the Subscriber's Entrust Certificate changes or if a change in circumstances would make the information in the Subscriber's Entrust Certificate misleading or inaccurate; or (2) there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key in the Entrust Certificate;
(viii) all use of the Entrust Certificate shall cease upon expiration or revocation of such certificate;
(ix) the Entrust Certificate will not be used for any hazardous or unlawful (including tortious) activities; and
(x) the subject named in the Entrust Certificate corresponds to the Subscriber.

2.1.4 Relying Party Obligations

Relying Parties shall, in accordance with the applicable requirements of this CPS:

(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 this CPS and the Relying Party Agreement;
(iii) trust and make use of an Entrust Certificate only if the Entrust Certificate has not expired or been revoked and if a proper chain of trust can be established to a trustworthy root;

(iv) trust and make use of an Entrust Certificate only if verified on a Supported Platform; and

(v) 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 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

In addition to any other Relying Party obligations in the Acrobat End User License Agreement, Entrust hereby provides notice to all Relying Parties that reliance on a CDS-signed document is only permitted if verified on a Supported Platform (as identified in the Adobe CP). This notice is also included in the User Notice field within each Certificate published by Entrust.

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 a revoked or expired Entrust Certificate;

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

(iv) the Relying Party shall not rely on an Entrust Certificate unless verified on a Supported Platform;

(v) 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;

(v) the Relying Party shall not use an Entrust Certificate for any hazardous or unlawful (including tortious) activities; and

(vi) the Relying Party shall not unreasonably rely on any Entrust Certificate having regard to this CPS, including without limit the limitations of liability set forth in this CPS at §2.2 (including all subsections of such section).

2.1.5 Repository Obligations

Entrust will make available, in accordance with this CPS, Entrust Certificate revocation information published by the Entrust CA.

2.2 Liability

In this §2.2 (including all subsections):

- the Entrust Group is defined to mean Entrust, Inc. and all of its subsidiaries, including any subcontractors, distributors, agents, suppliers, employees or directors of any of the foregoing; and
- the Adobe Root CA has the meaning set forth in the Adobe CP.

The Entrust Group and the Adobe Root CA are express third party beneficiaries of this §2.2 (including all subsections).

2.2.1 Warranty Disclaimers

In addition to any other warranty disclaimers in the Subscriber Agreement or the Adobe CP, except as expressly set forth in this CPS or the Adobe CP, the Entrust Group and the Adobe Root CA disclaim any and all warranties related to any certificates issued in the CDS PKI, including warranties:

(i) related to the accuracy, authenticity, reliability, completeness, currentness, merchantability, or fitness of any information contained in certificates or otherwise compiled, published, or disseminated by or on behalf of any entities other than the Entrust CA or the Adobe Root CA;
(ii) related to the security provided by any cryptographic process implemented by any entities other than the Adobe Root CA or the Entrust CA;
(iii) for representations of information contained in a certificate;
(iv) of non-repudiation of any messages; and
(v) related to any software or applications.

THE ENTRUST GROUP AND THE ADOBE ROOT CA SPECIFICALLY DISCLAIM ANY AND ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SATISFACTORY QUALITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE.

2.2.2 Limitations on CA Liability

Under no circumstances will the Entrust Group or the Adobe Root CA be liable to any purported Relying Parties, or any other person or entity, for any loss of use, revenue or profit, lost or damaged data, or other commercial or economic loss or for any other direct, indirect, incidental, special, punitive, exemplary or consequential damages whatsoever, even if advised of the possibility of such damages or if such damages are foreseeable. This limitation shall apply even in the event of a fundamental breach or a breach of the fundamental terms of this CPS.

Except as expressly provided for in the Adobe CP, the Adobe Root CA accepts no responsibility or liability for any transactions relying upon certificates issued by Entrust.

Except as expressly provided for in this CPS, the Entrust Group accepts no responsibility or liability for any transactions relying upon certificates issued by any person other than Entrust.

IN NO EVENT SHALL THE TOTAL CUMULATIVE LIABILITY OF THE ENTRUST GROUP TO ANY APPLICANT, SUBSCRIBER, RELYING PARTY OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION ARISING OUT OF OR RELATING TO ANY ENTRUST CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO ENTRUST CERTIFICATES, INCLUDING ANY USE OR RELIANCE ON ANY ENTRUST CERTIFICATE, EXCEED FIVE THOUSAND UNITED STATES DOLLARS ($5000.00 U.S.) ("CUMULATIVE DAMAGE CAP"). THIS LIMITATION SHALL APPLY ON A PER ENTRUST CERTIFICATE BASIS REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CAUSES OF ACTION ARISING OUT OF OR RELATED TO SUCH ENTRUST CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO SUCH ENTRUST CERTIFICATE. THE FOREGOING LIMITATIONS SHALL APPLY TO ANY LIABILITY WHETHER BASED IN CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), LEGISLATION OR ANY OTHER THEORY OF LIABILITY,

INCLUDING ANY DIRECT, INDIRECT, SPECIAL, STATUTORY, PUNITIVE, EXEMPLARY, CONSEQUENTIAL, RELIANCE, OR INCIDENTAL DAMAGES.

IN THE EVENT THAT LIABILITY TO ANY PARTY ARISING OUT OF OR RELATING TO AN ENTRUST CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO AN ENTRUST CERTIFICATE EXCEEDS THE CUMULATIVE DAMAGE CAP SET FORTH IN THIS SECTION ABOVE, THE AMOUNTS AVAILABLE UNDER THE CUMULATIVE DAMAGE CAP SHALL BE APPORTIONED FIRST TO THE EARLIEST CLAIMS TO ACHIEVE FINAL DISPUTE RESOLUTION UNLESS OTHERWISE ORDERED BY A COURT OF COMPETENT JURISDICTION. IN NO EVENT SHALL THE ENTRUST GROUP BE OBLIGATED TO PAY MORE THAN THE CUMULATIVE DAMAGE CAP FOR ANY ENTRUST CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO AN ENTRUST CERTIFICATE REGARDLESS OF APPORTIONMENT AMONG CLAIMANTS.

THE FOREGOING LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN AND EVEN IF THE ENTRUST GROUP OR THE ADOBE CA HAVE BEEN ADVISED OF THE POSSIBILITY OF THOSE DAMAGES.

SOME JURISDICTIONS DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, SO THESE LIMITATIONS SET FORTH ABOVE MAY NOT APPLY TO CERTAIN APPLICANTS, SUBSCRIBERS, RELYING PARTIES, OR OTHER PERSONS, ENTITIES, OR ORGANIZATIONS.

THE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND THE LIMITATIONS OF LIABILITY IN THIS CPS CONSTITUTE AN ESSENTIAL PART OF THIS CPS, AND SUBSCRIBER AGREEMENTS.

ALL APPLICANTS, SUBSCRIBERS, RELYING PARTIES, AND OTHER PERSONS, ENTITIES, AND ORGANIZATIONS ACKNOWLEDGE THAT BUT FOR THESE DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, AND CONDITIONS AND LIMITATIONS OF LIABILITY, ENTRUST WOULD NOT ISSUE ENTRUST CERTIFICATES TO SUBSCRIBERS AND THAT THESE PROVISIONS PROVIDE FOR A REASONABLE ALLOCATION OF RISK.

2.3 Financial Responsibility

In this §2.3 (including all subsections):

- the Entrust Group is defined to mean Entrust, Inc. and all of its subsidiaries, including any subcontractors, distributors, agents, suppliers, employees or directors of any of the foregoing; and
- the Adobe Root CA has the meaning set forth in the Adobe CP.

The Entrust Group and the Adobe Root CA are express third party beneficiaries of this §2.3 (including all subsections).

2.3.1 Indemnification by Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ADOBE AND THE ENTRUST GROUP (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 THIS CPS, THE SUBSCRIBER AGREEMENT, ANY RELYING PARTY AGREEMENT, THE ADOBE CP, 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 ADOBE AND THE ENTRUST GROUP (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 THIS CPS, THE SUBSCRIBER AGREEMENT, ANY RELYING PARTY AGREEMENT, THE ADOBE CP, 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 CPS, or in any Subscriber Agreement, or any Relying Party Agreement, or in the Adobe CP shall be deemed to make the Entrust Group or the Adobe Root CA 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 either Entrust and any other third party. Nothing in this CPS, or in any Subscriber 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 of the Entrust Group or the Adobe Root CA.

2.3.3 Administrative Processes

No Stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The laws of the Province of Ontario, Canada, excluding its conflict of laws rules, shall govern the construction, validity, interpretation, enforceability and performance of this CPS, all Subscriber Agreements and all Relying Party Agreements. The application of the United Nations Convention on Contracts for the International Sale of Goods to this CPS, any Subscriber Agreements, and any Relying Party Agreements is expressly excluded. Any dispute arising out of or in respect to this CPS, any Subscriber Agreement, any Relying Party Agreement, or in respect to any Entrust Certificate or any services provided in respect to any Entrust Certificate 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

Neither Entrust nor RAs operating under the authority of the Entrust CA, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall 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 this CPS, any Subscriber 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 CPS to "§" refer to the sections of this CPS. As used in this 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 CPS as a whole, as the same may from time to time be amended or supplemented, and not to any subdivision contained in this 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 this CPS, any Subscriber 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 this CPS, any Subscriber 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 this CPS, any Subscriber 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 THIS CPS, ANY SUBSCRIBER 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 THIS CPS, ANY SUBSCRIBER 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 §2.1, §2.2 (including all subsections), §2.3 (including all subsections), §2.4, §2.8, §2.9, §3.1.5, §3.1.6, §4.6 and §8.1 shall survive termination or expiration of this CPS, any Subscriber Agreements, and any Relying Party Agreements. All references to sections that survive termination of this CPS, any Subscriber Agreements, and any Relying Party Agreements, shall include all sub-sections of such sections. All payment obligations shall survive any termination or expiration of this CPS, any Subscriber Agreements, and any Relying Party Agreements.

2.4.2.3 Merger

This CPS, the Subscriber Agreements, and the Relying Party Agreements state all of the rights and obligations of Entrust, any RAs operating under the Entrust CA, any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing, and 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 Entrust, any RAs operating under the Entrust CA, any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, and directors of any of the foregoing 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 a conflict between the provisions of this CPS and any express written agreement between Entrust or an RA operating under the Entrust CA and a Subscriber or Relying Party, with respect to Entrust Certificates or any services provided in respect to Entrust Certificates, such other express written agreement shall take precedence. In the event of any inconsistency between the provisions of this CPS and the provisions of any Subscriber Agreement or any Relying Party Agreement, this CPS shall govern.

2.4.2.5 Waiver

The failure of Entrust to enforce, at any time, any of the provisions of this CPS, a Subscriber 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 CPS, a Subscriber 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 CPS, a Subscriber 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 RA or Reseller operating under the Entrust CA ("Registration Authority") to enforce, at any time, any of the provisions of this CPS, any Subscriber 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 CPS, any Subscriber 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 Subscriber 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 CPS, a Subscriber 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 this CPS, any Subscriber 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 this CPS, any Subscriber Agreement, or any Relying Party Agreement are personal to the Applicant, Subscriber, or Relying Party that entered into the Subscriber 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 this CPS, any Subscriber Agreement, or any Relying Party Agreement. Entrust may assign, sell, transfer, or otherwise dispose of this CPS, any Subscriber Agreements, or any Relying Party Agreements together with all of its rights and obligations under this CPS, any Subscriber 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 this CPS, the Subscriber 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 this CPS, or in any Subscriber 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 this CPS, any Subscriber 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 this CPS, any Subscriber 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 RAs, 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. This CPS and various other related information is published in the Entrust Repository. This 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) current and past versions of this CPS for Adobe CDS;
(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

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

2.6.3 Access Controls

This CPS is published in the Entrust Repository. This 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 CPS. The Entrust Repositories are the only approved source for CRL and other information about Entrust Certificates.

2.7 Compliance Audit

Entrust Certification Authorities will undergo an annual compliance audit in accordance with the then-current WebTrust for CA audit program as published by the AICPA.

2.7.1 Frequency of Entity Compliance Audit

Entrust Certification Authorities, Entrust-operated Registration Authorities, and RAs operating under the Entrust Certification Authorities shall be audited once per calendar year for compliance with the practices and procedures set forth in this CPS. If the results of an audit report recommend remedial action, Entrust or the applicable RA 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 and who is currently licensed to perform WebTrust for CA audits.

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. this CPS for Adobe CDS; 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 the Entrust CA, 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 RAs 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 CPS, a Subscriber Agreement, or a Relying Party Agreement. Entrust and all RAs 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 this CPS, a Subscriber 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 an Entrust Certificate and that Entrust and all RAs 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 RAs 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 RAs 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 this CPS shall not be considered confidential. Without limiting the foregoing, information that (i) was or becomes known through no fault of Entrust, an RA under an Entrust Certification Authority, a Reseller, or a Co-marketer, (ii) was rightfully known or becomes rightfully known to Entrust, an RA 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 RA 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, RAs 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, RAs 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 RA, 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, RAs 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 this CPS, the Subscriber's Subscriber 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 this CPS, the Subscriber's Subscriber 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 this CPS provided that (i) the copyright notice on the first page of this CPS is retained on any copies of this CPS, and (ii) this CPS is reproduced fully and accurately. Entrust retains all right, title, and interest (including all intellectual property rights), in, to and under this CPS.

In no event shall Entrust or an RA operating under the authority of the Entrust CA, or any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing 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

The Subject names in an Entrust 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 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;
(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 an individual not associated with an organization, the organization name can be the name of the Applicant; and
(iii) "Common Name" (CN) which may be an individual's name, an organization's name or the name of a specific role within an organization.

All attributes are as defined in ITU-T Recommendation X.521.

3.1.2 Need for Names to Be Meaningful

Names used in Entrust Certificates must be meaningful in that they can be understood and used by Relying Parties and linked to a Subscriber, an Organization or a specific individual operating in a certain role.

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 the Entrust CA 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. This 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 the Entrust CA or between a third-party complainant and an Entrust Certification Authority or a Registration Authority operating under the Entrust CA 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 Certificate 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 the Entrust CA 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 the Entrust CA 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 the Entrust CA may initiate the following actions. The Entrust Certification Authority or the Registration Authority operating under the Entrust CA 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 the Entrust CA 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 CPS, a Subscriber Agreement, or any Relying Party Agreement. During any litigation, an Entrust Certification Authority will not revoke and a Registration Authority

operating under the Entrust CA 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 CPS, a Subscriber 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 this CPS, the Subscriber's Subscriber Agreement, and the Relying Party's Relying Party Agreement.

Registration Authorities operating under the Entrust CA 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

Applicants generating their own private keys must prove possession of that private key by using it to sign a certificate request and providing that request to the Issuing CA. The Entrust Certification Authority will validate the signature using the Applicant's public key.

3.1.8 Authentication of Organizational Identity

Authentication of the Organization Identity will apply to applicants requesting Entrust Certificate for use on behalf of an Organization.

An Organizational Representative will be required to submit an application including the following information:

- Organization Name, Address, City/Locality, State/Province and Country
- Organization Representative Name,
- Organization Representative Phone Number,
- Organization Representative E-mail Address

The Organization Representative must identify and authorize the individuals who will act as the Local Registration Authority on behalf of the Organization. The Local Registration Authority will be responsible for approving authorized applicants for Entrust Certificate.

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 according to the requirements of this CPS. Registration Authorities operating under the Entrust Certification Authorities shall determine whether the organizational identity and address provided with an Entrust Certificate Application are consistent with information contained in third-party databases and/or governmental sources. An application for an Entrust Certificate shall only be approved if the organizational identity information provided can be confirmed to be consistent with the appropriate third-party databases and/or governmental sources.

3.1.9 Authentication of Individual Identity

Authentication of the Individual Identity will apply to applicants requesting an Entrust Certificate for individual use and not associated with an Organization. Registration Authorities operating under the Entrust Certification Authorities shall perform a limited verification of any individual identities that are submitted by an Applicant or Subscriber according to the requirements of this CPS.

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.

3.2 Routine Rekey

Each Entrust Certificate shall contain a Certificate expiration date. Entrust does not renew Entrust Certificate, accordingly, 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 shall be required to complete the initial application process, as described in §4.1, including generation of a new Key Pair and submission of the new Public Key Pair of this Key Pair with the Entrust Certificate Application.

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 destroy the Private Key corresponding to the Public Key contained in the Subscriber's Entrust Certificate in accordance with §6.2.9.

3.3 Rekey After Revocation

Entrust Certification Authorities and Registration Authorities operating under Entrust Certification Authorities do not renew Entrust Certificate 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.

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 requiring the pass phrase submitted by the Subscriber with the Entrust Certificate Application and/or some subset of the information provided by the Subscriber with the Entrust Certificate Application. Upon receipt and confirmation of such information, the Registration Authority shall then process the revocation request as stipulated in §4.4.

4 Operational Requirements

4.1 Certificate Application

To obtain an Entrust Certificate, an Applicant must:

(i) generate a secure and cryptographically sound Key Pair on a cryptographic device that meets or exceeds FIPS-140 Level 2 certification standards,
(ii) agree to all of this CPS and the Subscriber Agreement, and
(iii) complete and submit an Entrust Certificate Application, providing all information requested by an Entrust-operated Registration Authority or by an RA 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 this CPS and the Subscriber Agreement, an Entrust-operated Registration Authority or a RA operating under the Entrust CA shall follow the procedures described in §3.1.8 and §3.1.9 to perform a 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.

4.2 Certificate Issuance

After performing limited verification of the information provided by an Applicant with an Entrust Certificate Application according to the requirements of this CPS, a Registration Authority operating under the Entrust CA may request that an Entrust Certification Authority issue an Entrust Certificate. Upon receipt of a request from a Registration Authority operating under the Entrust CA, 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 RA operating under the authority of the Entrust CA, 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

The Applicant shall review and verify the accuracy of the contents of the Entrust Certificate. If the contents of the Entrust Certificate are inaccurate, the Applicant shall immediately advise the Registration Authority; otherwise the Entrust Certificate shall be deemed to be accepted. The Entrust Certificate shall also be deemed to be accepted by the Applicant upon first use.

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 the Entrust CA 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 the Entrust CA 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 the Entrust CA 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) receipt of a revocation request from the Adobe Policy Authority;

(ii) Compromise of such Entrust Certification Authority's Private Key or Compromise of a superior Certification Authority's Private Key;
(iii) breach by the Subscriber of any of the terms of this CPS or the Subscriber's Subscriber Agreement;
(iv) any change in the information contained in an Entrust Certificate issued to a Subscriber;
(v) non-payment of any Entrust Certificate fees or service fees;
(vi) a determination that an Entrust Certificate was not issued in accordance with the requirements of this CPS or the Subscriber's Subscriber Agreement;
(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 Certificate 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 Certificate; or
(ix) 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 causes 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 CPS, the Subscriber's Subscriber 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 the Entrust CA 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. An Entrust Certification Authority shall be entitled to revoke and shall revoke a Subscriber's Entrust Certificate upon receipt of a revocation request from an authorized representative of the Adobe Policy Authority.

4.4.3 Procedure for Revocation Request

A Registration Authority operating under the Entrust CA shall authenticate a request by a Subscriber for revocation of their Entrust Certificate by requiring (i) a subset of the information provided by the Subscriber with the Subscriber's Entrust Certificate Application that would allow a reasonable person to determine that the requester is the Subscriber, or (ii) the pass phrase submitted by the Subscriber with the Subscriber's Entrust Certificate Application or (iii) verification by a contact at the Subscriber. 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 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 applicable 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 for Entrust Certificates issued to end entities at least once every seven days.

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 at least once every 24 hours to determine whether the Entrust Certificate that the Relying Party wishes to rely on has been revoked. In no event shall Adobe, Entrust, or any RAs operating under the Entrust CA, or any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing 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 and On-line Certificate Status Protocol (OCSP).

Entrust Certification Authorities shall sign and make available OCSP responses for Entrust Certificates issued to end entities at least once every four days. OCSP responses will have a maximum expiration time of ten days.

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

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 destroy the Private Key corresponding to the Public Key contained in the Subscriber's Entrust Certificate in accordance with §6.2.9. 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.

4.4.16 Time Stamp Server

All digital signatures created by Entrust Certificates will include a trusted time stamp issued from an RFC 3161 compliant Time Stamp Authority (TSA) server. The TSA certificate is issued by the Entrust Certification Authority for Adobe CDS which issued the Entrust Certificate used to apply the digital signature.

4.5 Security Audit Procedures

4.5.1 Types of Event Recorded

Significant security events in the Entrust Certification Authorities are automatically time-stamped and recorded as audit logs in audit trail files.

The Entrust Certification Authorities and all Registration Authorities operating under the Entrust CA 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 Certificate; 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.

4.5.2 Frequency of Processing Log

The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis.

4.5.3 Retention Period for Audit Log

Audit logs are maintained for a minimum of 7 years.

4.5.4 Protection of Audit Log

The audit log is stored in operating system flat files. Each audit log file consists of an audit header that contains information about the audits in the file and list of events. A Message Authentication Code (MAC) is created for each of the audit events and the audit header. Each audit log file has a different key used to generate the MAC. The CA key is used to protect the audit key, which is stored in the audit header.

4.5.5 Audit Log Backup Procedures

Audit trail files are regularly backed up and sent offsite for storage in a secure archive facility

4.5.6 Audit Collection System

No stipulation.

4.5.7 Notification to Event-Causing Subject

No stipulation.

4.5.8 Vulnerability Assessments

The Entrust Certification Authority monitors anomalies and attempts to violate the integrity of the system, including the equipment, its physical location, and its personnel.

4.6 Records Archival

4.6.1 Types of Events Records

Archive Records
Certification Practice Statement
Contractual obligations
System and equipment configuration
Modifications and updates to system or configuration
Revocation requests
Subscriber identity Authentication data.
Documentation of receipt and acceptance of certificates
All certificates issued or published
A complete listing of all certificates revoked
All Audit Logs
Other data or applications to verify archive contents
Documentation required by compliance auditors

4.6.2 Retention Period of Archive

The audit trail files, databases and revocation information for Entrust Certification Authorities are both 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

4.6.3 Protection of Archive

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.

4.6.4 Archive Backup Procedures

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 location.

4.6.5 Requirements for Time-stamping of Records

No stipulation.

4.6.6 Archive Collection System

No stipulation.

4.6.7 Procedures to Obtain and Verify Archive Information

Requests for access to the archives must be authorized by the Entrust Certificate Authority. For approved requests, the CA obtains the requested archive materiel or accompanies the requestor to the archive facility.

4.7 Key Changeover

Entrust Certification Authorities will be retired from service at the end of their respective lifetimes as defined in §6.3. New Certification Authorities with new key pairs will be created as required to support the continuation of Entrust Certification Authority Services. Each Entrust Certification Authority will continue to sign and publish CRLs until the end of the CA certificate lifetime. The Certification Authority termination 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 or loss of facility. In the event of facility loss, the Adobe Policy Authority will be notified immediately.

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. Such policies include investigation of the compromise, determination of the root cause, and implementation of appropriate measures to address the causes. Detailed procedures to address key compromise are documented in the Entrust Certification Authority operating procedures.

At a minimum, all Subscribers and the Adobe Policy Authority 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. The Adobe Policy Authority will be notified prior to any termination of services for Entrust Certificates.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

5.1.1 Site Location and Construction

The computing facilities that host the Entrust Certificate Authority services are located within the Entrust Ottawa, Canada facility. 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. The Security zone is constructed slab-to-slab with drywall and wire mesh. The Security zone is protected by electronic control access systems, alarmed doors and is monitored via a 24x7 recorded security camera and motion detector system.

5.1.2 Physical Access

Entrust employees a four zone security model to protect physical access to the CA:
1. Reception Zone – all Entrust employees
2. Customer Service Zone – CA, RA and supporting operational personnel
3. Registration Authority Zone – two factor, limited to employees with RA or CA trusted roles
4. Certification Authority (Security) Zone – two factor, dual access controlled zone, limited to employees with CA trusted roles

The system controlling physical access to the Certificate Authority zone requires a minimum of two persons to enter the zone, and a minimum of two persons to exit the zone, enforcing the requirement that no single person can access the room at any time. Access to the room is logged and the logs are reviewed on a regular basis. Alarm systems are used to notify security personnel of any violation of the rules for access to the Certification Authority Zone.

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

Backups for key systems are captured and retained as follows:

- Backups are performed daily and kept for at least 4 weeks.
- Every week, on-site backups (containing one week's data) are sent off site to a secure location and stored there for 3 weeks.
- Every 5 weeks, the weekly backup is retained for 7 years.

Backup copies of security items required to recover the CA, such as passwords, tokens and keys, are stored offsite in a safety deposit box under dual-person control.

5.2 Procedural Controls

5.2.1 Trusted Roles

The CA application is represented by the Entrust Authority Security Manager software. The main administrative interfaces to the CA application are Security Manager Administration and Master Control. These interfaces are used by End Entities with special privileges to perform the duties of trusted roles in the CA.

The trusted roles that make up the CA Service are:

- CA Service Manager;
- Deputy CA Service Manager;
- Entrust Certificate Services Security Officer;
- RA Administrator;
- Verification Specialist;
- Verification Manager; and
- Support Specialist.

A trusted role supporting the operation of the CA Service infrastructure is the

- Network and Operating System Administrator

The Entrust roles consist of:

- Master User;
- Security Officer;
- Entrust Administrator; and
- Directory Administrator.

The division of responsibilities and assignment of Entrust roles to trusted CA personnel ensures the separation of duties to prevent situations where a single individual would be able to seriously compromise the CA Service. All activities can be tracked to individuals.

5.2.2 Number of Persons Required per Task

Physical and logical multi-person controls are implemented for sensitive CA operations as follows:

- At least two trusted CA personnel are required to access the room where the Entrust Authority software is located
- Access privileges for the Entrust Authority software are assigned such that at least two trusted CA personnel are required
- Sensitive security items such as keys, tokens and copies of passwords are stored under dual control.
- Sensitive operations within the Entrust Authority software require two trusted CA personnel to complete

5.2.3 Identification and Authentication for Each Role

Prior to being assigned to a CA trusted role, CA operational personnel must undergo background investigations. Roles are authorized and assigned to personnel by the CA Service Manager. Assignment of privilege accesses associated with each role is authorized by the CA Service Manager.

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 the Entrust Certification Authority issuing Entrust Certificates was created during an audited key generation ceremony and witnessed by an independent third-party, as defined in §2.7.3. The Entrust Certification Authority Key Pair was generated in cryptographic hardware that meets FIPS 140-1 Level 3 certification standards.

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 medium that prevents exportation or duplication and that meets or exceed FIPS 140-1 Level 2 certification standards.

Temporary key pairs and corresponding Certificates for Adobe CDS may be generated by the Entrust Certification Authority for the limited purpose of testing such Certificates for Adobe CDS. The test Certificates for Adobe CDS must not contain actual identities and must be clearly marked for testing purposes only. These temporary test key pairs are exempt from the requirement that cryptographic hardware must meet or exceed FIPS 140-1 Level 2 or 3 certification standards.

6.1.2 Private Key Delivery to Entity

Subscriber private keys must be generated by the Subscriber or provided to the Subscriber by an Authorized Representative. An Authorized Representative shall be designated by an Organization Representative to perform the Local Registration Authority (LRA) in accordance with this Certificate Practice Statement. Furthermore, the LRA subsequent to identity verification of the Subscriber may securely hold the Subscriber's private key under the following conditions:

(i) The Subscriber has explicitly agreed to proxy the responsibility of private key protection;

(ii) The Organization Representative has identified the Authorized Representative as an LRA in a letter of authorization submitted to the Entrust Certification Authority; and

(iii) The Authorized Representative agrees to accept the full responsibilities of private key protection and authorized use as defined by this Certificate Practice Statement.

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 Certificates 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.

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

6.1.5 Key Sizes

The Entrust Certification Authority uses an RSA key pair of 2048 bits.
Subscriber Certificates for Adobe CDS shall use an RSA key pair with at least 2048 bits.

6.1.6 Public-Key Parameters Generation

No stipulation.

6.1.7 Parameter Quality Checking

No stipulation.

6.1.8 Hardware/Software Key Generation

Key generation must meet the requirements of §6.1.1 and §6.1.5.

6.1.9 Key Usage Purposes

Entrust Certificate 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.

6.2 Private Key Protection

6.2.1 Standards for Cryptographic Module

The Entrust Certification Authorities use Entrust Authority software in conjunction with hardware certified to FIPS 140-1 Level 3 to protect the Entrust Certification Authorities' Private Keys.

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 (a) meet or exceed FIPS 140-1 Level 2 standards or (b) for which the cryptographic hardware module manufacturer has applied for FIPS 140-1 Level 2 status within the previous year without receiving a notice of noncompliance or other communication indicating that such device fails to meet such standard. The Entrust Certificate Authority does not back up Subscriber's private keys.

Entrust Certificate Authority may provide a cryptographic hardware module to the Subscriber. The cryptographic hardware modules are secured with limited access and the serial number is recorded before they are sent to the Subscriber. The cryptographic hardware modules are shipped in an empty state without including the private key. Private keys are generated on the cryptographic hardware module by the Subscriber.

Temporary key pairs generated by the Entrust Certification Authority for testing purposes pursuant to §6.1.1 are exempt from the requirement of using cryptographic hardware that meets or exceeds FIPS 140-1 Level 2 or 3 certification standards.

6.2.2 Private Key (n out of m) Multi-person Control

Entrust Certification Authorities use 2 out of 6 multi-person controls on Certification Authority private keys where one person must be assigned the role of Master User. Particularly sensitive operations require a second Master User.

6.2.3 Private Key Escrow

Private keys shall not be escrowed.

6.2.4 Private Key Backup

Backups of the Entrust Certification Authorities' Private Keys were made during the initial installation and setup of the Entrust Authority software and are stored on FIPS 140-1 Level 3 tokens. The backup tokens are held in secure facilities under two-person control.

Backups of Subscribers' private keys shall not be made.

6.2.5 Private Key Archival

Private keys shall not be archived.

6.2.6 Private Key Entry into Cryptographic Module

Private keys are either generated by the Cryptographic Module or securely imported to it.

6.2.7 Method of Activating Private Key

In order to activate a private key, Subscribers or Trusted Roles must authenticate to the medium housing the private key. Forms of authentication include but are not limited to passwords, PINs, pass-phrases, and biometrics.

6.2.8 Method of Deactivating Private Key

Private keys must be deactivated when not in use. Forms of deactivation include but are not limited to logout and physical removal of cryptographic module. Procedures for deactivation of private keys may be prescribed by the manufacturer of the cryptographic module.

6.2.9 Method of Destroying Private Key

Secure procedures for the destruction of private keys as prescribed by the manufacturer of the cryptographic module shall be followed when a private key is no longer needed or the CDS Certificate to which it corresponds has expired or has been revoked.

6.3 Other Aspects of Key Pair Management

The maximum lifetime for Entrust Certification Authorities' Key Pairs is 20 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

Data used to activate private keys shall have an appropriate level of strength for keys being protected. Subscriber created activation data (e.g. strong password) or stronger access controls (e.g. biometrics) shall be used.

6.4.2 Activation Data Protection

Activation data shall be protected from disclosure. Activation data should not be written down. Cryptographic hardware shall have a mechanism to lock the hardware (at least temporarily) after a certain number of failed attempts to login.

6.4.3 Other Aspects of 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 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

Entrust Certification Authorities employ appropriate security measures to ensure that the CA is protected from intrusion and other attacks that could render it inoperative.

6.8 Cryptographic Module Engineering Controls

See §6.2.1.

7 Certificate and CRL Profiles

The profile for the Entrust Certificate and Certificate Revocation List (CRL) issued by an Entrust Certification Authority conform to the specifications contained in the IETF RFC 3280 Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile.

7.1 Entrust Certificate Profile

The following X.509 version 3 Certificate profile is used by the Entrust Certification Authorities for Certificates for Adobe CDS:

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Attributes		
Version		v3
SerialNumber		integer: unique serial number within the name space of the issuing Entrust Certification Authority
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		CN = Entrust CA for Adobe, OU = (c) 2008 Entrust, Inc. OU = www.entrust.net/CPS is incorporated by reference O = Entrust, Inc., C = US
Validity		Maximum validity period is 5 years
Subject		Based application information
SubjectPublicKeyInfo		• rsaEncryption – {1.2.840.113549.1.1.1} RSA public key is 2048 bit public key
Extensions		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages • Digital Signature • Key Encipherment
CertificatePolicies	Critical	1.2.840.113583.1.2.1 User Notice: This Certification Practice Statement (CPS) for Adobe Certified Document Services (CDS) available at www.entrust.net/CPS is hereby incorporated into your use or reliance on this Certificate. This CPS contains limitations on warranties and liabilities. Reliance on a CDS-signed document is only permitted if verified on a Supported Platform (as

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
		identified in the Adobe Certificate Policy). Copyright (c) 2008 Entrust Limited.
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	http://crl.entrust.net/adobeca.crl

The following X.509 version 3 Certificate profile is used by the Entrust Certification Authorities for Test Certificates for Adobe CDS:

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
Attributes		
Version		v3
SerialNumber		integer: unique serial number within the name space of the issuing Entrust Certification Authority
Signature		sha-1 w/ RSAEncryption – {1.2.840.113549.1.1.5}
Issuer		CN = Entrust CA for Adobe, OU = (c) 2008 Entrust, Inc. OU = www.entrust.net/CPS is incorporated by reference O = Entrust, Inc., C = US
Validity		Maximum validity period is 90 days
Subject		Based application information
SubjectPublicKeyInfo		• rsaEncryption – {1.2.840.113549.1.1.1} RSA public key is 2048 bit public key
Extensions		
AuthorityKeyIdentifier	Non-critical	contains a 20 byte SHA-1 hash of the SUB-Root CA public key
KeyUsage	Critical	Minimum Key Usages • Digital Signature • Key Encipherment
CertificatePolicies	Critical	1.2.840.113583.1.2.1 User Notice: This Certification Practice Statement (CPS) for Adobe Certified Document Services (CDS) available at www.entrust.net/CPS is hereby incorporated into your use or reliance on this Certificate. This CPS contains limitations on warranties and liabilities.

X.509 v3 Certificate Attributes/ Extensions	Critical / Non Critical	Value / Notes
		Reliance on a CDS-signed document is only permitted if verified on a Supported Platform (as identified in the Adobe Certificate Policy). Copyright (c) 2008 Entrust Limited.
ExtendedKeyUsage	Non-critical	1.2.840.113583.1.1.5
CRLDistributionPoints	Non-critical	http://crl.entrust.net/adobeca.crl

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
- user certificate: Certificate serial number of a revoked certificate
- revoked certificates: list of revoked Certificate information

The following CRL and CRL entry extensions are used by the Entrust Certification Authorities:

- Authority Key Identifier: Contains a 20 byte hash of the CA certificate's subject public key information field
- CRL Number: A CRL number, which is unique to each CRL issued.

7.3 OCSP Profile

The profile for the Entrust 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.

8 Specification Administration

8.1 Specification Change Procedures

Entrust may, in its discretion, modify this CPS and the terms and conditions contained herein from time to time. Modifications to this CPS that, in the judgment of a reasonable person, will have little or no impact on Adobe, Applicants, Subscribers, and Relying Parties, may be made with no change to this CPS version number and no notification to Applicants, Subscribers, and Relying Parties, provided, however, that notice is provided to Adobe. Such changes shall become effective immediately upon publication in the Entrust Repository.

Modifications to this CPS that, in the judgment of a reasonable person may have a significant impact on Adobe, Applicants, Subscribers, and Relying Parties, 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 CPS prior to such effective date. Such publication to the Entrust Repository shall not occur until Adobe reviews and approves the modified CPS. In the event that Entrust makes a significant modification to CPS, the version number of this 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 this CPS becomes effective, such Subscriber shall be deemed to have consented to the terms and conditions of such updated version of this CPS and shall be bound by the terms and conditions of such updated version of this CPS.

8.2 Publication and Notification Policies

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

8.3 CPS Approval Procedures

This CPS and any subsequent changes shall be approved by the Entrust Policy Authority and Adobe. The Entrust Policy Authority will ensure that this CPS and any subsequent changes are in compliance with the Adobe CDS Certificate Policy.

9 Acronyms

CA	Certification Authority
CDS	Certified Document Services
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DN	Distinguished Name
DNS	Domain Name Server
DSA	Digital Signature Algorithm
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
ITU-T	International Telecommunication Union - Telecommunication Standardization Sector
MAC	Message Authentication Code
OCSP	Online Certificate Status Protocol
OA	Operational Authority
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
URL	Universal Resource Locator

10 Definitions

Adobe: means Adobe Systems Incorporated.

Adobe Policy Authority: means selected members of Adobe's management team responsible for the management of the Adobe CDS Certificate Policy.

Affiliate: means Entrust, and any corporation or other entity that Entrust directly or indirectly controls. 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.

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.

Authorized Representative: see Local Registration Authority

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 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 the Entrust CA the right to promote Entrust Certificates.

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

CPS: means this document.

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 Group: means Entrust, Inc. and all of its subsidiaries, including any subcontractors, distributors, agents, suppliers, employees or directors of any of the foregoing.

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 CPS: See CPS.

Entrust Certificate: means a Certificate issued by an Entrust Certification Authority for digitally signing and verifying Adobe Acrobat documents.

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

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, this CPS, and other information and agreements that are intended to govern the use of Entrust Certificates.

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.

Local Registration Authority: means a representative of the Organization authorized to perform the Registration Authority function for the Organization.

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.

Organizational Representative: means a representative of the Organization with the authority to contractually bind the Organization

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 verification of information provided by the Subject following the requirements of this CPS. In the event that the information provided by a Subject satisfies the criteria specified in this CPS, 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.

Relying Party Agreement: means the agreement between a Relying and Entrust or between a Relying Party and an RA 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 the Entrust CA 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.

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.

Subscriber Agreement: means the agreement between a Subscriber and Entrust or between a Subscriber and an RA 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.

Supported Platform: means those applications specified on the CDS information web page, currently http://www.adobe.com/security/partners_cds.html.

