ENTRUST CERTIFICATE SERVICES

Certification Practice Statement

for SSL Web Server Certificates

Version: 2.1
August 1, 2007

Revision History

Issue	Date	Changes in this Revision
1.0	May 26, 1999	Initial version.
2.0	July 1, 2000	Addition of provisions dealing with subordinate entities (such as third party registration authorities) in the Entrust.net SSL Web Server public key infrastructure. Revision of numerous other terms and conditions.
2.01	May 30, 2001	Minor revisions having no substantive impact.
2.02	January 1, 2002	Minor revisions related to replacement Cross Certificate.
2.03	January 1, 2003	Entrust legal name change.
2.04	August 20, 2003	Minor revisions related to use of certificates on more than one server; permitting use of asterisk in Subject name
2.05	November 28, 2003	Minor revisions to language to handle licensing issues.
2.06	May 14, 2004	Minor revisions to language for export requirements.
2.1	August 1, 2007	Minor revisions to ensure consistency with the CPS for EV SSL Certificates and to add OCSP references.

TABLE OF CONTENTS

1. Introduction

The Entrust Certificate Services Secure Sockets Layer (SSL) Web Server Certification Authorities issue Entrust SSL Web Server Certificates to support more secure communications between World Wide Web servers and browsers using the Secure Sockets Layer protocol. 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.

1.1 Overview

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

1.2 Identification

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

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

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

The following OID has been registered by the Entrust SSL Web Server CA for inclusion in SSL Web Server Certificates:

1.2.840.113533.7.75.2

1.3 Community and Application

Use of Entrust SSL Web Server Certificates is restricted to World Wide Web servers using the Secure Sockets Layer protocol. Any other use of Entrust SSL Web Server Certificates is prohibited.

1.3.1 Certification Authorities

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

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

1.3.2 Registration Authorities

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

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

1.3.3 End Entities

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

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

Additionally, certain licensors of Entrust are third party beneficiaries of this CPS and all agreements into which it is incorporated, including Microsoft Corporation.

1.3.4 Applicability

This Entrust Certificate Services SSL Web Server Certification Practice Statement is applicable to Entrust SSL Web Server Certificates issued by Entrust SSL Web Server Certification Authorities. SSL Web Server Certificates are intended for use in establishing web-based data communication conduits via TLS/SSL protocols.

Entrust SSL Web Server Certificates conform to the requirements of the ITU-T X.509 v3 standard with SSL extensions.

The primary purpose of an SSL Web Server Certificate is to facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a website.

1.4 Contact Details

1.4.1 Specification Administration Organization

The Entrust Certificate Services SSL Web Server Certification Practice Statement is administered by the Entrust Policy Authority; it is based on the policies established by Entrust Limited .

1.4.2 Contact Person

The contact information for questions about Entrust SSL Web Server Certificates is:

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

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

An Entrust SSL Web Server Certification Authority shall:

(i) provide Certification Authority services in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement;

(ii) upon receipt of a request from a Registration Authority operating under such Entrust SSL Web Server Certification Authority, issue an Entrust SSL Web Server Certificate in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement;

(iii) make available Entrust SSL Web Server Certificate revocation information by issuing Entrust SSL Web Server Certificates and by issuing and making available Entrust SSL Web Server Certificate CRLs in an Entrust Repository in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement;

(iv) issue and publish Entrust SSL Web Server Certificate CRLs on a regular schedule in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement; and

(v) upon receipt of a revocation request from a Registration Authority operating under such Entrust SSL Web Server Certification Authority, revoke the specified Entrust SSL Web Server Certificate in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement.

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

2.1.2 Registration Authority Obligations

A Registration Authority operating under an Entrust SSL Web Server Certification Authority shall:

(i) receive Entrust SSL Web Server Certificate Applications in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement;

(ii) perform limited verification of information submitted by Applicants when applying for Entrust SSL Web Server Certificates, and if such verification is successful, submit a request to an Entrust SSL Web Server Certification Authority for the issuance of an Entrust SSL Web Server Certificate, all in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement;

(iii) receive and verify requests from Subscribers for the revocation of Entrust SSL Web Server Certificates, and if the verification of a revocation request is successful, submit a request to an Entrust SSL Web Server Certification Authority for the revocation of such Entrust SSL Web Server Certificate, all in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement;

(iv) notify Subscribers, in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement, that an Entrust SSL Web Server Certificate has been issued to them; and

(v) notify Subscribers, in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement, that an Entrust SSL Web Server Certificate issued to them has been revoked or will soon expire.

Entrust may use one or more representatives or agents to perform its obligations in respect of an Entrust-operated Registration Authority under the Entrust SSL Web Server Certification Practice Statement, any

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

2.1.3 Subscriber Obligations

Subscribers and Applicants shall:

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

(ii) provide, in any communications with Entrust or an independent third-party Registration Authority, correct information with no errors, misrepresentations, or omissions;

(iii) generate a new, secure, and cryptographically sound Key Pair to be used in association with the Subscriber's Entrust SSL Web Server Certificate or Applicant's Entrust SSL Web Server Certificate Application;

(iv) read and agree to all terms and conditions of the Entrust SSL Web Server Certification Practice Statement and Subscription Agreement;

(v) refrain from modifying the contents of an Entrust SSL Web Server Certificate;

(vi) use Entrust SSL Web Server Certificates exclusively for legal and authorized purposes in accordance with the terms and conditions of the Entrust SSL Web Server Certification Practice Statement and applicable laws;

(vii) only use an Entrust SSL Web Server Certificate on behalf of the person, entity, or organization listed as the Subject in such Entrust SSL Web Server Certificate;

(viii) keep confidential and properly protect the Subscriber's or Applicant's Private Keys;

(ix) notify Entrust or, if Applicant submitted its Entrust SSL Web Server Certificate Application to an independent third-party Registration Authority, such independent third-party Registration Authority, as soon as reasonably practicable of any change to any information included in the Applicant's Entrust SSL Web Server Certificate Application or any change in any circumstances that would make the information in the Applicant's Entrust SSL Web Server Certificate Application misleading or inaccurate;

(x) notify Entrust or, if Subscriber received its Entrust SSL Web Server Certificate through an independent third-party Registration Authority, such independent third-party Registration Authority, as soon as reasonably practicable of any change to any information included in the Subscriber's Entrust SSL Web Server Certificate or any change in any circumstances that would make the information in the Subscriber's Entrust SSL Web Server Certificate misleading or inaccurate;

(xi) immediately cease to use an Entrust SSL Web Server Certificate if any information included in the Subscriber's Entrust SSL Web Server Certificate or if any change in any circumstances would make the information in the Subscriber's Entrust SSL Web Server Certificate misleading or inaccurate;

(xii) notify Entrust or, if Subscriber received its Entrust SSL Web Server Certificate from an independent third-party Registration Authority, such independent third-party Registration Authority, immediately of any suspected or actual Compromise of the Subscriber's or Applicant's Private Keys and request the revocation of such Entrust SSL Web Server Certificate;

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

(xiv) only install the Subscriber's Entrust SSL Web Server Certificate on one (1) of Subscriber's World Wide Web server and only use such Entrust SSL Web Server Certificate in connection with such server unless, otherwise expressly permitted by Entrust in writing;

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

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

Entrust SSL Web Server Certificates and related information may be subject to export, import, and/or use restrictions. Subscribers shall comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use Entrust SSL Web Server Certificates 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 SSL Web Server Certificates or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with Entrust SSL Web Server Certificates may be subject to export, import, and/or use restrictions. Subscribers shall comply with all laws and regulations applicable to a Subscriber's right to export, import, and/or use such Technology or related information. Subscribers shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

2.1.3.1 Subscriber and Applicant Representations and Warranties

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

(i) all information provided to Entrust or to any independent third-party Registration Authorities, both in the SSL Web Server Certificate Request and as otherwise requested by Entrust in connection with the issuance of the SSL Web Server 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 SSL Web Server 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 independent third-party Registration Authorities in connection with an Entrust SSL Web Server 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 SSL Web Server Certificate(s) shall not be installed or used until it has reviewed and verified the accuracy of the data in each SSL Web Server Certificate;

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

(vi) Entrust shall be immediately notified if any information included in the Entrust SSL Web Server Certificate Application changes or if any change in any circumstances would make the information in the Entrust SSL Web Server Certificate Application misleading or inaccurate;

(vii) all use of the Entrust SSL Web Server Certificate and its associated private key shall cease immediately, and the Subscriber will promptly request the revocation of the Entrust Web Server SSL Certificate, if (1) any information included in the Subscriber's Entrust SSL Web Server Certificate changes or if any change in any circumstances would make the information in the Subscriber's Entrust SSL Web Server Certificate misleading or inaccurate; or (2) there is any actual or suspected misue or compromise of the Private Key associated with the Public Key in the Entrust Web Server SSL Certificate;

(viii) all use of the Entrust SSL Web Server Certificate shall cease upon expiration or revocation of such Entrust SSL Web Server Certificate and such Entrust SSL Web Server Certificate shall be removed from the devices and/or software in which it has been installed; and

(vii) the Entrust SSL Web Server Certificates will not be used for any hazardous or unlawful (including tortious) activities.

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

(ix) the Subscriber has the exclusive right to use the domain name listed in the Entrust SSL Web Server Certificate;

2.1.3.2 Subscriber Notice Requirements

Subscriber shall display the following notice in a prominent location on Subscriber's World Wide Web site that may be viewed by Relying Parties (for example, in the "legal" or "disclaimers" section of Subscriber's World Wide Web site):

> "Reliance on Entrust SSL Web Server Certificates is governed by the terms and conditions of the Entrust SSL Web Server Certification Practice Statement (located at www.entrust.net/CPS) and by the Relying Party Agreement (located at www.entrust.net/CPS). Reliance on an Entrust SSL Web Server Certificate shall constitute acceptance of the terms and conditions of the Entrust SSL Web Server Certification Practice Statement and the Relying Party Agreement."

2.1.4 Relying Party Obligations

Relying Parties shall:

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

(ii) read and agree to all terms and conditions of the Entrust SSL Web Server Certification Practice Statement and the Relying Party Agreement;

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

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

(v) make their own judgment and rely on an Entrust SSL Web Server 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 SSL Web Server Certificate and the value of any transaction that may involve the use of an Entrust SSL Web Server Certificate.

Entrust SSL Web Server 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 SSL Web Server 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 SSL Web Server Certificates and/or related information. Certain cryptographic techniques, software, hardware, and firmware ("Technology") that may be used in processing or in conjunction with Entrust SSL Web Server Certificates may be subject to export, import, and/or use restrictions. Relying Parties shall comply with all laws and regulations applicable to a Relying Party's right to export, import, and/or use such Technology or related information. Relying Parties shall be responsible for procuring all required licenses and permissions for any export, import, and/or use of such Technology or related information.

2.1.4.1 Relying Party Representations and Warranties

Relying Parties represent and warrant to Entrust that:

(i) the Relying Party shall properly validate an Entrust SSL Web Server Certificate before making a determination about whether to rely on such Entrust SSL Web Server Certificate, including confirmation that the Entrust SSL Web Server 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 SSL Web Server Certificate;

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

(iv) the Relying Party shall exercise its own judgment in determining whether it is reasonable under the circumstances to rely on an Entrust SSL Web Server Certificate, including determining whether such reliance is reasonable given the nature of the security and trust provided by an Entrust SSL Web Server Certificate and the value of any transaction that may involve the use of an Entrust SSL Web Server Certificate; and

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

2.1.5 Repository Obligations

An Entrust Repository shall:

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

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

2.2 Liability

THE MAXIMUM CUMULATIVE LIABILITY OF ENTRUST, ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, RESELLERS, CO-MARKETERS OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES OR

DIRECTORS OF ANY OF THE FOREGOING TO ANY APPLICANTS, SUBSCRIBERS, RELYING PARTIES OR ANY OTHER PERSONS, ENTITIES, OR ORGANIZATIONS FOR ANY LOSSES, COSTS, EXPENSES, LIBILITIES, DAMAGES, CLAIMS, OR SETTLEMENT AMOUNTS ARISING OUT OF OR RELATING TO USE OF AN ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO ANY ENTRUST SSL WEB SERVER CERTIFICATES IS LIMITED BY THIS ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT. THIS ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT ALSO CONTAINS LIMITED WARRANTIES, LIMITATIONS ON LIABILITY, AND DISCLAIMERS OF REPRESENTATIONS, WARRANTIES AND CONDITIONS.

2.2.1 CA Liability

2.2.1.1 Warranties and Limitations on Warranties

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

(i) Entrust SSL Web Server Certification Authorities shall provide Repository services consistent with the practices and procedures set forth in this Entrust SSL Web Server Certification Practice Statement;

(ii) Entrust SSL Web Server Certification Authorities shall perform Entrust SSL Web Server Certificate issuance consistent with the procedures set forth in this Entrust SSL Web Server Certification Practice Statement; and

(iii) Entrust SSL Web Server Certification Authorities shall provide revocation services consistent with the procedures set forth in this Entrust SSL Web Server Certification Practice Statement.

Notwithstanding the foregoing, in no event does Entrust, any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing make any representations, or provide any warranties, or conditions to any Applicants, Subscribers, Relying Parties, or any other persons, entities, or organizations with respect to (i) the techniques used in the generation and storage of the Private Key corresponding to the Public Key in an Entrust SSL Web Server Certificate, including, whether such Private Key has been Compromised or was generated using sound cryptographic techniques, (ii) the reliability of any cryptographic techniques or methods used in conducting any act, transaction, or process involving or utilizing an Entrust SSL Web Server Certificate, (iii) any software whatsoever, or (iv) non-repudiation of any Entrust SSL Web Server Certificate or any transaction facilitated through the use of an Entrust SSL Web Server Certificate, since such determination is a matter of applicable law.

Applicants, Subscribers, and Relying Parties acknowledge and agree that operations in relation to Entrust SSL Web Server Certificates and Entrust SSL Web Server Certificate Applications are dependent on the transmission of information over communication infrastructures such as, without limitation, the Internet, telephone and telecommunications lines and networks, servers, firewalls, proxies, routers, switches, and bridges ("Telecommunication Equipment") and that this Telecommunication Equipment is not under the control of Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing. Neither Entrust nor any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall be liable for any error, failure, delay, interruption, defect, or corruption in relation to an Entrust SSL Web Server Certificate, an Entrust SSL Web Server Certificate CRL, Entrust SSL OCSP message, or an Entrust SSL Web Server Certificate Application to the extent that such error, failure, delay, interruption, defect, or corruption is caused by such Telecommunication Equipment.

2.2.1.2 Disclaimers

EXCEPT AS SPECIFICALLY PROVIDED IN SECTION 2.2.1.1, NEITHER ENTRUST NOR ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITY OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, NOR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING MAKE ANY REPRESENTATIONS OR GIVE ANY WARRANTIES OR CONDITIONS, WHETHER EXPRESS, IMPLIED, STATUTORY, BY USAGE OF TRADE, OR OTHERWISE, AND ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, AND DIRECTORS OF ANY OF THE FOREGOING SPECIFICALLY DISCLAIM ANY AND ALL REPRESENTATIONS, WARRANTIES, AND CONDITIONS OF MERCHANTABILITY, NON-INFRINGEMENT, TITLE, SATISFACTORY QUALITY, AND/OR FITNESS FOR A PARTICULAR PURPOSE.

2.2.1.3 Loss Limitations

IN NO EVENT SHALL THE TOTAL CUMULATIVE LIABILITY OF ENTRUST, ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITY OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, ANY RESELLERS, OR CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING TO ANY APPLICANT, SUBSCRIBER, RELYING PARTY OR ANY OTHER PERSON, ENTITY, OR ORGANIZATION ARISING OUT OF OR RELATING TO ANY ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO ENTRUST SSL WEB SERVER CERTIFICATES, INCLUDING ANY USE OR RELIANCE ON ANY ENTRUST SSL WEB SERVER CERTIFICATE, EXCEED ONE THOUSAND UNITED STATES DOLLARS ($1000.00 U.S.) ("CUMULATIVE DAMAGE CAP"). THIS LIMITATION SHALL APPLY ON A PER ENTRUST SSL WEB SERVER CERTIFICATE BASIS REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CAUSES OF ACTION ARISING OUT OF OR RELATED TO SUCH ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO SUCH ENTRUST SSL WEB SERVER 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 ARISING OUT OF OR RELATING TO AN ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICES PROVIDED IN RESPECT TO AN ENTRUST SSL WEB SERVER 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 ENTRUST OR ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITY OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, OR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING BE OBLIGATED TO PAY MORE THAN THE CUMULATIVE DAMAGE CAP FOR ANY ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICES PROVIDED IN RESEPCT TO AN ENTRUST SSL WEB SERVER CERTIFICATE REGARDLESS OF APPORTIONMENT AMONG CLAIMANTS.

IN NO EVENT SHALL ENTRUST OR ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITY OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, OR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS,

DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING BE LIABLE FOR ANY INCIDENTAL, SPECIAL, STATUTORY, PUNITIVE, EXEMPLARY, INDIRECT, RELIANCE, OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS, LOSS OF BUSINESS OPPORTUNITIES, LOSS OF GOODWILL, LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF DATA, LOST SAVINGS OR OTHER SIMILAR PECUNIARY LOSS) WHETHER ARISING FROM CONTRACT (INCLUDING FUNDAMENTAL BREACH), TORT (INCLUDING NEGLIGENCE), LEGISLATION OR ANY OTHER THEORY OF LIABILITY.

THE FOREGOING LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY STATED HEREIN AND EVEN IF ENTRUST OR ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITY OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, OR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING 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 ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT CONSTITUTE AN ESSENTIAL PART OF THE ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT, ANY SUBSCRIPTION AGREEMENTS, AND ANY RELYING PARTY 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 SSL WEB SERVER CERTIFICATES TO SUBSCRIBERS AND NEITHER ENTRUST NOR ANY ANY INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, NOR ANY RESELLERS, CO-MARKETERS, OR ANY SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING WOULD PROVIDE SERVICES IN RESPECT TO ENTRUST SSL WEB SERVER CERTIFICATES AND THAT THESE PROVISIONS PROVIDE FOR A REASONABLE ALLOCATION OF RISK.

2.2.1.4 Other Exclusions

Without limitation, neither Entrust nor any independent third-party Registration Authorities operating under an Entrust SSL Web Server Certification Authority, nor any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall be liable to any Applicants, Subscribers, Relying Parties or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to use of an Entrust SSL Web Server Certificate or any services provided in respect to an Entrust SSL Web Server Certificate if:

(i) the Entrust SSL Web Server Certificate was issued as a result of errors, misrepresentations, or other acts or omissions of a Subscriber or of any other person, entity, or organization;
(ii) the Entrust SSL Web Server Certificate has expired or has been revoked;
(iii) the Entrust SSL Web Server Certificate has been modified or otherwise altered;
(iv) the Subscriber failed to stop using an Entrust SSL Web Server Certificate after the information contain in such Entrust SSL Web Server Certificate changed or after circumstances changed so that the information contained in such Entrust SSL Web Server Certificate became misleading or inaccurate;

(v) a Subscriber breached the Entrust SSL Web Server Certification Practice Statement or the Subscriber's Subscription Agreement, or a Relying Party breached the Entrust SSL Web Server Certification Practice Statement or the Relying Party's Relying Party Agreement;

(vi) the Private Key associated with the Entrust SSL Web Server Certificate has been Compromised; or

(vii) the Entrust SSL Web Server Certificate is used other than as permitted by the Entrust SSL Web Server Certification Practice Statement or is used in contravention of applicable law.

In no event shall Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable to any Applicant, Subscriber, or any other person, entity, or organization for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to the refusal by Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing to issue or request the issuance of an Entrust SSL Web Server Certificate. In no event shall Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable to any Applicant, Subscriber, or any other person, entity, or organization for any losses, costs, liabilities, expenses, damages, claims, or settlement amounts arising out of or relating to any delay by Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing, in issuing or in requesting the issuance of an Entrust SSL Web Server Certificate.

In no event shall Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing be liable to any Subscriber, Relying Party, or any other person, entity, or organization for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or relating to any proceeding or allegation that an Entrust SSL Web Server Certificate or any information contained in an Entrust SSL Web Server Certificate infringes, misappropriates, dilutes, unfairly competes with, or otherwise violates any patent, trademark, copyright, trade secret, or any other intellectual property right or other right of any person, entity, or organization in any jurisdiction.

2.2.1.5 Hazardous Activities

Entrust SSL Web Server Certificates and the services provided by Entrust in respect to Entrust SSL Web Server Certificates are not designed, manufactured, or intended for use in or in conjunction with hazardous activities or uses requiring fail-safe performance, including the operation of nuclear facilities, aircraft navigation or communications systems, air traffic control, medical devices or direct life support machines. Entrust and any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, and any Resellers, Co-marketers, and any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing specifically disclaim any and all representations, warranties, and conditions with respect to such uses, whether express, implied, statutory, by usage of trade, or otherwise.

2.2.2 RA Liability

The same liability provisions that apply in Section 2.2.1 with respect to Entrust SSL Web Server Certification Authorities shall apply with respect to Entrust-operated Registration Authorities and independent third-party Registration Authorities operating under Entrust SSL Web Server Certification Authorities and all Resellers, Co-marketers and all subcontractors, distributors, agents, suppliers, employees, and directors of any of the foregoing.

2.3 Financial Responsibility

Subscribers and Relying Parties shall be responsible for the financial consequences to such Subscribers, Relying Parties, and to any other persons, entities, or organizations for any transactions in which such Subscribers or Relying Parties participate and which use Entrust SSL Web Server Certificates or any services provided in respect to Entrust SSL Web Server Certificates. Entrust makes no representations and gives no warranties or conditions regarding the financial efficacy of any transaction completed utilizing an Entrust SSL Web Server Certificate or any services provided in respect to Entrust SSL Web Server Certificates and neither Entrust nor any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, nor any Resellers, Co-marketers, nor any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall have any liability except as explicitly set forth herein in respect to the use of or reliance on an Entrust SSL Web Server Certificate or any services provided in respect to Entrust SSL Web Server Certificates.

2.3.1 Indemnification by Relying Parties

RELYING PARTIES SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, AND DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY USE OR RELIANCE BY A RELYING PARTY ON ANY ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO ENTRUST SSL WEB SERVER CERTIFICATES, INCLUDING (I) LACK OF PROPER VALIDATION OF AN ENTRUST SSL WEB SERVER CERTIFICATE BY A RELYING PARTY, (II) RELIANCE BY THE RELYING PARTY ON AN EXPIRED OR REVOKED ENTRUST SSL WEB SERVER CERTIFICATE, (III) USE OF AN ENTRUST SSL WEB SERVER CERTIFICATE OTHER THAN AS PERMITTED BY THE ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A RELYING PARTY TO EXERCISE REASONABLE JUDGMENT IN THE CIRCUMSTANCES IN RELYING ON AN ENTRUST SSL WEB SERVER CERTIFICATE, OR (V) ANY CLAIM OR ALLEGATION THAT THE RELIANCE BY A RELYING PARTY ON AN ENTRUST SSL WEB SERVER CERTIFICATE OR THE INFORMATION CONTAINED IN AN ENTRUST SSL WEB SERVER CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, RELYING PARTIES SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERT'S FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

2.3.1.1 Indemnification by Subscribers

SUBSCRIBERS SHALL INDEMNIFY AND HOLD ENTRUST AND ALL INDEPENDENT THIRD-PARTY REGISTRATION AUTHORITIES OPERATING UNDER AN ENTRUST SSL WEB SERVER CERTIFICATION AUTHORITY, AND ALL RESELLERS, CO-MARKETERS, AND ALL SUBCONTRACTORS, DISTRIBUTORS, AGENTS, SUPPLIERS, EMPLOYEES, OR DIRECTORS OF ANY OF THE FOREGOING (COLLECTIVELY, THE "INDEMNIFIED PARTIES") HARMLESS FROM AND AGAINST ANY AND ALL LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISING OUT OF OR RELATING TO ANY RELIANCE

BY A RELYING PARTY ON ANY ENTRUST SSL WEB SERVER CERTIFICATE OR ANY SERVICE PROVIDED IN RESPECT TO ENTRUST SSL WEB SERVER CERTIFICATES, INCLUDING ANY (I) ERROR, MISREPRESENTATION OR OMISSION MADE BY A SUBSCRIBER IN USING OR APPLYING FOR AN ENTRUST SSL WEB SERVER CERTIFICATE, (II) MODIFICATION MADE BY A SUBSCRIBER TO THE INFORMATION CONTAINED IN AN ENTRUST SSL WEB SERVER CERTIFICATE, (III) USE OF AN ENTRUST SSL WEB SERVER CERTIFICATE OTHER THAN AS PERMITTED BY THE ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT, THE SUBSCRIPTION AGREEMENT, ANY RELYING PARTY AGREEMENT, AND APPLICABLE LAW, (IV) FAILURE BY A SUBSCRIBER TO TAKE THE NECESSARY PRECAUTIONS TO PREVENT LOSS, DISCLOSURE, COMPROMISE OR UNAUTHORIZED USE OF THE PRIVATE KEY CORRESPONDING TO THE PUBLIC KEY IN SUCH SUBSCRIBER'S ENTRUST SSL WEB SERVER CERTIFICATE, OR (V) ALLEGATION THAT THE USE OF A SUBSCRIBER'S ENTRUST SSL WEB SERVER CERTIFICATE OR THE INFORMATION CONTAINED IN A SUBSCRIBER'S ENTRUST SSL WEB SERVER CERTIFICATE INFRINGES, MISAPPROPRIATES, DILUTES, UNFAIRLY COMPETES WITH, OR OTHERWISE VIOLATES THE RIGHTS INCLUDING INTELLECTUAL PROPERTY RIGHTS OR ANY OTHER RIGHTS OF ANYONE IN ANY JURISDICTION. NOTWITHSTANDING THE FOREGOING, A SUBSCRIBER SHALL NOT BE OBLIGATED TO PROVIDE ANY INDEMNIFICATION TO AN INDEMNIFIED PARTY IN RESPECT TO ANY LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS AND EXPERTS FEES) TO THE EXTENT THAT SUCH LIABILITIES, LOSSES, COSTS, EXPENSES, DAMAGES, CLAIMS, AND SETTLEMENT AMOUNTS (INCLUDING REASONABLE ATTORNEY'S FEES, COURT COSTS, AND EXPERT'S FEES) ARISE OUT OF OR RELATE TO ANY WILLFUL MISCONDUCT BY SUCH INDEMNIFIED PARTY.

2.3.2 Fiduciary Relationships

Nothing contained in this Entrust SSL Web Server Certification Practice Statement, or in any Subscription Agreement, or any Relying Party Agreement shall be deemed to constitute either Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing, 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 or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing and any Subscriber, Applicant, Relying Party or any other person, entity, or organization, for any purpose whatsoever. Nothing in the Entrust SSL Web Server Certification Practice Statement, or in any Subscription Agreement or any Relying Party Agreement shall confer on any Subscriber, Applicant, Relying Party, or any other third party, any authority to act for, bind, or create or assume any obligation or responsibility, or make any representation on behalf of Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, or any Resellers, Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing.

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 the Entrust SSL Web Server Certification Practice Statement, all Subscription Agreements and all Relying Party Agreements. The application of the United Nations Convention on Contracts for the International Sale of Goods to the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreements, and any Relying

Party Agreements is expressly excluded. Any dispute arising out of or in respect to the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreement, any Relying Party Agreement, or in respect to any Entrust SSL Web Server Certificates or any services provided in respect to any Entrust SSL Web Server Certificates that is not resolved by alternative dispute resolution, shall be brought in the provincial or federal courts sitting in Ottawa, Ontario, and each person, entity, or organization hereby agrees that such courts shall have personal and exclusive jurisdiction over such disputes. In the event that any matter is brought in a provincial or federal court, Applicants, Subscribers, and Relying Parties waive any right that such Applicants, Subscribers, and Relying Parties may have to a jury trial.

2.4.1.1 Force Majeure

Neither Entrust nor any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, 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 the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreement, or any Relying Party Agreement due to any causes beyond its reasonable control, which causes include acts of God or the public enemy, riots and insurrections, war, accidents, fire, strikes and other labor difficulties (whether or not Entrust is in a position to concede to such demands), embargoes, judicial action, failure or default of any superior certification authority, lack of or inability to obtain export permits or approvals, necessary labor, materials, energy, utilities, components or machinery, acts of civil or military authorities.

2.4.1.2 Interpretation

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

2.4.2 Severability, Survival, Merger, Notice

2.4.2.1 Severability

Whenever possible, each provision of the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreements, and any Relying Party Agreements shall be interpreted in such a manner as to be effective and valid under applicable law. If the application of any provision of the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreements, or any Relying Party Agreements or any portion thereof to any particular facts or circumstances shall be held to be invalid or unenforceable by an arbitrator or court of competent jurisdiction, then (i) the validity and enforceability of such provision as applied to any other particular facts or circumstances and the validity of other provisions of the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreements, or any Relying Party Agreements shall not in any way be affected or impaired thereby, and (ii) such provision shall be enforced to the maximum extent possible so as to effect its intent and it shall be reformed without further action to the extent necessary to make such provision valid and enforceable.

FOR GREATER CERTAINTY, IT IS EXPRESSLY UNDERSTOOD AND AGREED THAT EVERY PROVISION OF THE ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT, ANY SUBSCRIPTION AGREEMENTS, OR ANY RELYING PARTY AGREEMENTS THAT DEAL WITH (I) LIMITATION OF LIABILITY OR DAMAGES, (II) DISCLAIMERS OF REPRESENTATIONS, WARRANTIES, CONDITIONS, OR LIABILITIES, OR (III) INDEMNIFICATION, IS EXPRESSLY INTENDED TO BE SEVERABLE FROM ANY

OTHER PROVISIONS OF THE ENTRUST SSL WEB SERVER CERTIFICATION PRACTICE STATEMENT, ANY SUBSCRIPTION AGREEMENTS, OR ANY RELYING PARTY AGREEMENTS AND SHALL BE SO INTERPRETED AND ENFORCED.

2.4.2.2 Survival

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

2.4.2.3 Merger

The Entrust SSL Web Server Certification Practice Statement, the Subscription Agreements, and the Relying Party Agreements state all of the rights and obligations of Entrust, any independent third-party Registration Authorities operating under an Entrust SSL Web Server Certification Authority, 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 independent third-party Registration Authorities operating under an Entrust SSL Web Server Certification Authority, 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 the Entrust SSL Web Server Certification Practice Statement and any express written agreement between Entrust or an independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority and a Subscriber or Relying Party, with respect to Entrust SSL Web Server Certificates or any services provided in respect to Entrust SSL Web Server Certificates, such other express written agreement shall take precedence. In the event of any inconsistency between the provisions of this Entrust SSL Web Server Certification Practice Statement and the provisions of any Subscription Agreement or any Relying Party Agreement, the terms and conditions of this Entrust SSL Web Server Certification Practice Statement shall govern.

2.4.2.5 Waiver

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

Web Server Certification Practice Statement, any Subscription Agreement with such Registration Authority, or any Relying Party Agreement with such Registration Authority shall in no way be construed to be a present or future waiver of such provisions, nor in any way affect the ability of such Registration Authority to enforce each and every such provision thereafter. The express waiver by a Registration Authority of any provision, condition, or requirement of a Subscription Agreement with such Registration Authority or a Relying Party Agreement with such Registration Authority shall not constitute a waiver of any future obligation to comply with such provision, condition, or requirement.

2.4.2.6 Notice

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

2.4.2.7 Assignment

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

2.4.3 Dispute Resolution Procedures

Any disputes between a Subscriber or an Applicant and Entrust or any third-party Registration Authorities operating under the Entrust Certification Authorities, or a Relying Party and Entrust or any third-party Registration Authorities operating under the Entrust Certification Authorities, shall be submitted to mediation in accordance with the Commercial Mediation Rules of the American Arbitration Association which shall take place in English in Ottawa, Ontario. In the event that a resolution to such dispute cannot be achieved through mediation within thirty (30) days, the dispute shall be submitted to binding arbitration. The arbitrator shall have the right to decide all questions of arbitrability. The dispute shall be finally settled by arbitration in accordance with the rules of the American Arbitration Association, as modified by this provision. Such arbitration shall take place in English in Ottawa, Ontario, before a sole arbitrator appointed by the American Arbitration Association (AAA) who shall be appointed by the AAA from its Technology Panel and shall be reasonably knowledgeable in electronic commerce disputes. The arbitrator

shall apply the laws of the Province of Ontario, without regard to its conflict of laws provisions, and shall render a written decision within thirty (30) days from the date of close of the arbitration hearing, but no more than one (1) year from the date that the matter was submitted for arbitration. The decision of the arbitrator shall be binding and conclusive and may be entered in any court of competent jurisdiction. In each arbitration, the prevailing party shall be entitled to an award of all or a portion of its costs in such arbitration, including reasonable attorney's fees actually incurred. Nothing in the Entrust SSL Web Server Certification Practice Statement, or in any Subscription Agreement, or any Relying Party Agreement shall preclude Entrust or any third-party Registration Authorities operating under the Entrust Certification Authorities from applying to any court of competent jurisdiction for temporary or permanent injunctive relief, without breach of this Section 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 SSL Web Server Certificate, or (ii) alleged breach of the terms and conditions of the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreement, or any Relying Party Agreement. The institution of any arbitration or any action shall not relieve an Applicant, Subscriber or Relying Party of its obligations under the Entrust SSL Web Server Certification Practice Statement, any Subscription Agreement, or any Relying Party Agreement.

2.4.3.1 Limitation Period on Arbitrations and Actions

Any and all arbitrations or legal actions in respect to a dispute that is related to an Entrust SSL Web Server Certificate or any services provided in respect to an Entrust SSL Web Server Certificate shall be commenced prior to the end of one (1) year after (i) the expiration or revocation of the Entrust SSL Web Server Certificate in dispute, or (ii) the date of provision of the disputed service or services in respect to the Entrust SSL Web Server Certificate in dispute, whichever is sooner. If any arbitration or action in respect to a dispute that is related to an Entrust SSL Web Server Certificate or any service or services provided in respect to an Entrust SSL Web Server 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 SSL Web Server Certificates are set forth in the Entrust Repository. These fees are subject to change, and any such changes shall become effective immediately after posting in the Entrust Repository. The fees for services provided by independent third-party Registration Authorities, Resellers and Co-marketers in respect to Entrust SSL Web Server 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 SSL Web Server Certificates or services provided in respect to Entrust SSL Web Server Certificates.

2.6 Publication and Repositories

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

2.6.1 Publication of CA Information

The following Entrust SSL Web Server Certificate information is published in the Entrust Repository:

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

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

2.6.2 Frequency of Publication

The Entrust SSL Web Server Certification Practice Statement may be re-issued and published in accordance with the policy set forth in Section 8.

2.6.3 Access Controls

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

2.7 Compliance Audit

2.7.1 Frequency of Entity Compliance Audit

Entrust SSL Web Server Certification Authorities, Entrust-operated Registration Authorities, and independent third-party Registration Authorities operating under the Entrust SSL Web Server Certification Authorities shall be audited once per calendar year for compliance with the practices and procedures set

forth in the Entrust SSL Web Server Certification Practice Statement. If the results of an audit report recommend remedial action, Entrust or the applicable independent third-party Registration Authority shall initiate corrective action within thirty (30) days of receipt of such audit report.

2.7.2 Identity/Qualifications of Auditor

The compliance audit shall be performed by a certified public accounting firm with a demonstrated competency in the evaluation of Certification Authorities and Registration Authorities. Deloitte & Touche LLP has been selected as the auditor for the Entrust Certification Authorities and for the Entrust-operated Registration Authorities.

2.7.3 Auditor's Relationship to Audited Party

The certified public accounting firm selected to perform the compliance audit for the Entrust SSL Web Server 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 SSL Web Server Certification Authorities, Entrust-operated Registration Authorities, or independent third-party operated Registration Authorities under the Entrust Certification Authorities against the policies and procedures set forth in:

i. the Entrust SSL Web Server Certification Practice Statement; 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 SSL Web Server Certification Authority, Entrust-operated Registration Authority, or independent third-party operated Registration Authority under an Entrust SSL Web Server 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 SSL Web Server Certification Authorities, to the Entrust Policy Authority, and, in the case of any Entrust-operated Registration Authorities under an Entrust SSL Web Server Certification Authorities, to the Entrust Policy Authority, and in the case of third-party Registration Authorities operating under an Entrust SSL Web Server Certification Authority, to the operational authority for such Registration Authority.

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

2.8 Confidentiality

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

2.8.1 Types of Information to be Kept Confidential

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

2.8.2 Types of Information not Considered Confidential

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

2.8.4 Release to Law Enforcement Officials

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

2.8.5 Release as Part of Civil Discovery

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

2.8.6 Disclosure Upon Owner's Request

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

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

In no event shall Entrust or any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, 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 SSL Web Server Certificate or arising from or relating to any services provided in relation to any Entrust SSL Web Server Certificate.

3 Identification and Authentication

3.1 Initial Registration

Before issuing an SSL Web Server Certificate, the Entrust SSL Web Server Certification Authorities ensure that all Subject organization information in the SSL Web Server Certificate conforms to the requirements of, and has been verified in accordance with, the procedures prescribed in this Certification Practice Statement 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 SSL Web Server Certificate comply with the X.501 Distinguished Name (DN) form. Entrust SSL Web Server Certification Authorities shall use a single naming convention as set forth below. Each Entrust SSL Web Server Certificate shall contain the following information:

(i) the "Country Name" (C) which is the two-letter ISO 3166 code for the country in which the Applicant is located and plans to host the World Wide Web server on which the Applicant is intending to install the Entrust SSL Web Server Certificate;
(ii) the "Organization Name" (O) which is the name of the organization in the case of a corporation, partnership, or other entity. In the case of a sole proprietorship, the organization name can be the name of the Applicant;
(iii) the "Organizational Unit Name" (OU) which is an optional field. The OU field may be used to distinguish between different organizational groups within an organization (for example, to distinguish between human resources, marketing, and development); and
(iv) the "Common Name" (CN) which is the fully qualified hostname or path used in the DNS of the World Wide Web server on which the Applicant is intending to install the Entrust SSL Web Server Certificate.

3.1.2 Need for Names to Be Meaningful

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

3.1.3 Rules for Interpreting Various Name Forms

Subject names for Entrust SSL Web Server Certificates shall be interpreted as set forth in Sections 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 World Wide Web servers to which it is issued. Each Entrust SSL Web Server Certificate shall be issued a unique serial number.

3.1.5 Name Claim Dispute Resolution Procedure

The Subject names in Entrust SSL Web Server Certificates are issued on a "first come, first served" basis. By accepting a Subject name for incorporation into an Entrust SSL Web Server Certificate, a Registration Authority operating under an Entrust SSL Web Server Certification Authority does not determine whether the use of such information infringes upon, misappropriates, dilutes, unfairly competes with, or otherwise violates any intellectual property right or any other rights of any person, entity, or organization. The Entrust Certification Authorities and any Registration Authorities operating under the Entrust Certification Authorities neither act as an arbitrator nor provide any dispute resolution between Subscribers or between Subscribers and third-party complainants in respect to the use of any information in an Entrust SSL Web

Server Certificate. The Entrust SSL Web Server Certification Practice Statement does not bestow any procedural or substantive rights on any Subscriber or third-party complainant in respect to any information in an Entrust SSL Web Server 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 SSL Web Server Certification Authority or a Registration Authority operating under an Entrust SSL Web Server Certification Authority or between a third-party complainant and an Entrust SSL Web Server Certification Authority or a Registration Authority operating under an Entrust SSL Web Server Certification Authority arising out of any information in an Entrust SSL Web Server Certificate. Entrust SSL Web Server Certification Authorities and Registration Authorities operating under Entrust SSL Web Server Certification Authorities shall respectively have the right to revoke and the right to request revocation of Entrust SSL Web Server Certificates upon receipt of a properly authenticated order from an arbitrator or court of competent jurisdiction requiring the revocation of an Entrust SSL Web Server Certificate.

3.1.6 Recognition, Authentication and Role of Trademarks

An Entrust SSL Web Server Certification Authority or a Registration Authority operating under an Entrust SSL Web Server Certification Authority may, in certain circumstances, take action in respect to an Entrust SSL Web Server 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 SSL Web Server Certification Authority or a Registration Authority operating under an Entrust SSL Web Server Certification Authority with (i) a certified copy that is not more than three (3) months old of a trademark registration from the principal trademark office in any one of the United States, Canada, Japan, Australia or any of the member countries of the European Union, and further provided that such registration is still in full force and effect, and (ii) a copy of a prior written notice to the Subscriber of the Entrust SSL Web Server Certificate in dispute, stating that the complainant believes that information in the Subscriber's Entrust SSL Web Server 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 SSL Web Server Certificate in dispute, an Entrust SSL Web Server Certification Authority or a Registration Authority operating under an Entrust SSL Web Server Certification Authority may initiate the following actions. The Entrust SSL Web Server Certification Authority or the Registration Authority operating under an Entrust SSL Web Server Certification Authority may determine whether the issue date of the Subscriber's Entrust SSL Web Server Certificate predates the registration date on the trademark registration provided by the complainant. If the date of issuance of the Subscriber's Entrust SSL Web Server Certificate predates the trademark registration date, the Entrust SSL Web Server Certification Authority or the Registration Authority operating under the Entrust SSL Web Server 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 SSL Web Server Certificate is after the registration date on the trademark registration provided by the complainant, the Entrust SSL Web Server Certification Authority or the Registration Authority operating under the Entrust SSL Web Server 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 SSL Web Server Certification Authority or the Registration Authority operating under the Entrust SSL Web Server 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 SSL Web Server Certification Authority and the Registration Authorities operating under that Entrust SSL Web Server Certification Authority respectively may revoke or may request revocation of the disputed Entrust SSL Web Server 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 SSL Web Server Certificate, and if the party instigating the litigation provides an Entrust SSL Web Server Certification Authority or a Registration Authority operating under an Entrust SSL Web Server Certification Authority with a copy of the file-stamped complaint or statement of claim, the Entrust SSL Web Server Certification Authority will maintain the current status of the Entrust SSL Web Server Certificate or the Registration Authority operating under the Entrust SSL Web Server Certification Authority will request that the Entrust SSL Web Server Certification Authority maintain the current status of the Entrust SSL Web Server Certificate, subject to any requirements to change the status of such Entrust SSL Web Server Certificate otherwise provided or required under this Entrust SSL Web Server Certification Practice Statement, a Subscription Agreement, or any Relying Party Agreement. During any litigation, an Entrust SSL Web Server Certification Authority will not revoke and a Registration Authority operating under an Entrust SSL Web Server Certification Authority will not request revocation of an Entrust SSL Web Server Certificate that is in dispute unless ordered by an arbitrator or a court of competent jurisdiction or as otherwise provided or required under this Entrust SSL Web Server Certification Practice Statement, a Subscription Agreement, or any Relying Party Agreement. In the event of litigation as contemplated above, Entrust SSL Web Server Certification Authorities and Registration Authorities operating under the Entrust SSL Web Server Certification Authorities will comply with any directions by a court of competent jurisdiction in respect to an Entrust SSL Web Server 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 SSL Web Server Certificate, Entrust and/or any third party operating a Registration Authority under an Entrust SSL Web Server 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 SSL Web Server Certificate shall remain subject to all of the terms and conditions of the Entrust SSL Web Server Certification Practice Statement, the Subscriber's Subscription Agreement, and the Relying Party's Relying Party Agreement.

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

3.1.7 Method to Prove Possession of Private Key

Registration Authorities perform proof of possession tests for CSRs created using reversible asymmetric algorithms (such as RSA) by validating the signature on the CSR submitted by the Applicant with the Entrust SSL Web Server Certificate Application.

3.1.8 Authentication of Organizational Identity

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

In the case of organizational identities that are not registered with any governmental sources, Registration Authorities operating under the Entrust SSL Web Server Certification Authorities shall use commercially reasonable efforts to confirm the existence of the organization. Such commercially reasonable efforts may include inquiries with banks or other trustworthy persons or institutions. Registration Authorities operating under the Entrust SSL Web Server Certification Authorities shall comply with all verification practices mandated by the Entrust Policy Authority.

The Entrust Policy Authority may, in its discretion, update verification practices to improve the organization identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the Entrust SSL Web Server Certification Practice Statement.

3.1.9 Authentication of Individual Identity

Registration Authorities operating under the Entrust SSL Web Server Certification Authorities shall perform a limited verification of any individual identities that are submitted by an Applicant or Subscriber. In order to establish the accuracy of an individual identity, the individual shall be required to appear before a representative of a Registration Authority operating under an Entrust SSL Web Server Certification Authority or a notary public in the jurisdiction of the Applicant. The individual shall be required to produce three (3) pieces of picture identification. The type of identification that is appropriate for proper identification shall be dependent on the jurisdiction of the Applicant.

The Entrust Policy Authority may, in its discretion, update verification practices to improve the individual identity verification process. Any changes to verification practices shall be published pursuant to the standard procedures for updating the Entrust SSL Web Server Certification Practice Statement.

3.2 Routine Rekey

Each Entrust SSL Web Server Certificate shall contain a Certificate expiration date. The reason for having an expiration date for a Certificate is to minimize the exposure of the Key Pair associated with the Certificate. For this reason, when processing a new Entrust SSL Web Server Certificate Application, Entrust requires that a new Key Pair be generated and that the new Public Key of this Key Pair be submitted with the Applicant's Entrust SSL Web Server Certificate Application. Entrust does not renew Entrust SSL Web Server Certificates, accordingly, if a Subscriber wishes to continue to use an Entrust SSL Web Server Certificate beyond the expiry date for the current Entrust SSL Web Server Certificate, the Subscriber must obtain a new Entrust SSL Web Server Certificate and replace the Entrust SSL Web Server Certificate that is about to expire. Subscribers submitting a new Entrust SSL Web Server Certificate Application will be required to complete the initial application process, as described in Section 4.1, including generation of a new Key Pair and submission of all information required for an initial application for an Entrust SSL Web Server Certificate. Processing of the SSL Web Server Certificate Application for re-key is handled as for an initial application as described in Sections 4.1 and 4.2.

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

3.3 Rekey After Revocation

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

3.4 Revocation Request

A Subscriber may request revocation of their Entrust SSL Web Server Certificate at any time provided that the Subscriber can validate to the Registration Authority that processed the Subscriber's Entrust SSL Web Server Certificate Application that the Subscriber is the person, organization, or entity to whom the Entrust SSL Web Server Certificate was issued. The Registration Authority shall authenticate a request from a Subscriber for revocation of their Entrust SSL Web Server Certificate by requiring the pass phrase submitted by the Subscriber with the Entrust SSL Web Server Certificate Application and/or some subset of the information provided by the Subscriber with the Entrust SSL Web Server Certificate Application. Upon receipt and confirmation of such information, the Registration Authority shall then process the revocation request as stipulated in Section 4.4.

4 Operational Requirements

4.1 Certificate Application

To obtain an Entrust SSL Web Server Certificate, an Applicant must:

(i) generate a secure and cryptographically sound Key Pair,
(ii) agree to all of the terms and conditions of the Entrust SSL Web Server Certification Practice Statement and the Subscription Agreement, and
(iii) complete and submit an Entrust SSL Web Server Certificate Application, providing all information requested by an Entrust-operated Registration Authority or by an independent third-party Registration Authority under an Entrust SSL Web Server Certification Authority (a "Registration Authority") without any errors, misrepresentation, or omissions.

Upon an Applicant's completion of the Entrust SSL Web Server Certificate Application and acceptance of the terms and conditions of this Entrust SSL Web Server Certification Practice Statement and the Subscription Agreement, a Entrust-operated Registration Authority or a independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority shall follow the procedures described in Sections 3.1.8 and 3.1.9 to perform limited verification of the information contained in the Entrust SSL Web Server 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 SSL Web Server Certificate from an Entrust SSL Web Server Certification Authority. If a Registration Authority refuses to request the issuance of an Entrust SSL Web Server 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 SSL Web Server Certificate Application.

In the event of successful verification of an Entrust SSL Web Server Certificate Application, the Registration Authority shall submit a request to an Entrust SSL Web Server Certification Authority for the issuance of an Entrust SSL Web Server Certificate and shall notify the Applicant by email once an Entrust SSL Web Server Certificate has been issued by the Entrust SSL Web Server Certification Authority. The Applicant will be provided with a URL that can be used to retrieve the Entrust SSL Web Server Certificate.

4.2 Certificate Issuance

Upon receipt of a request from a Registration Authority operating under an Entrust SSL Web Server Certification Authority, the Entrust SSL Web Server Certification Authority assigns a person who is not responsible for the collection of information to review all of the information and documentation assembled in support of the SSL Web Server Certificate Application and look for discrepancies or other details requiring further explanation. Upon successful completion of this Final Cross-Correlation and Due Diligence step, the Entrust SSL Web Server Certification Authority may generate and digitally sign an Entrust SSL Web Server Certificate in accordance with the Certificate profile described in Section 7.

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

4.3 Certificate Acceptance

Once an Entrust SSL Web Server Certificate has been generated and placed in an Entrust Repository, the Registration Authority that requested the issuance of the Entrust SSL Web Server Certificate shall use commercially reasonable efforts to notify the Applicant by email that the Applicant's Entrust SSL Web Server Certificate is available. The email will contain a URL for use by the Applicant to retrieve the Entrust SSL Web Server Certificate.

4.4 Certificate Suspension and Revocation

An Entrust SSL Web Server Certification Authority shall revoke an Entrust SSL Web Server Certificate after receiving a valid revocation request from a Registration Authority operating under such Entrust SSL Web Server Certification Authority. A Registration Authority operating under an Entrust SSL Web Server Certification Authority shall be entitled to request and may request that an Entrust SSL Web Server Certification Authority revoke an Entrust SSL Web Server Certificate after such Registration Authority receives a valid revocation request from the Subscriber for such Entrust SSL Web Server Certificate. A Registration Authority operating under an Entrust SSL Web Server Certification Authority shall be entitled to request and shall request that an Entrust SSL Web Server Certification Authority revoke an Entrust SSL Web Server Certificate if such Registration Authority becomes aware of the occurrence of any event that would require a Subscriber to cease to use such Entrust SSL Web Server Certificate. Entrust SSL Web Server Certification Authorities do not allow the suspension of Entrust SSL Web Server Certificates.

4.4.1 Circumstances for Revocation

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

(i) Compromise of such Entrust SSL Web Server Certification Authority's Private Key or Compromise of a superior Certification Authority's Private Key;
(ii) breach by the Subscriber of any of the terms of the Entrust SSL Web Server Certification Practice Statement or the Subscriber's Subscription Agreement;
(iii) any change in the information contained in an Entrust SSL Web Server Certificate issued to a Subscriber;
(iv) non-payment of any Entrust SSL Web Server Certificate fees or service fees;
(v) a determination that an Entrust SSL Web Server Certificate was not issued in accordance with the requirements of the Entrust SSL Web Server Certification Practice Statement or the Subscriber's Subscription Agreement;
(vi) the Entrust SSL Web Server Certification Authority receives notice or otherwise become aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the SSL Web Server Certificate, or that the Subscriber has failed to renew it domain name;
(vii) the Entrust SSL Web Server 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 SSL Web Server Certification Authority's jurisdiction of operation as described in Section 2.4;
(viii) the Entrust SSL Web Server Certification Authority ceases operations for any reason or the Entrust SSL Web Server Certification Authority's right to issue SSL Web Server Certificates expires or is revoked or terminated and the Entrust SSL Web Server Certification Authority has not arranged for another SSL Web Server Certification Authority to provide revocation support for the SSL Web Server Certificates; or
(ix) any other reason that may be reasonably expected to affect the integrity, security, or trustworthiness of an Entrust SSL Web Server Certificate or an Entrust SSL Web Server Certification Authority.

A Subscriber shall request revocation of their Entrust SSL Web Server 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 SSL Web Server Certificate request was not authorized and such authorization will not be retroactively granted;
(iii) change in the information contained in the Subscriber's Entrust SSL Web Server Certificate;

(iv) change in circumstances that causes the information contained in Subscriber's Entrust SSL Web Server 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 SSL Web Server Certificate Application. If a Subscriber's Entrust SSL Web Server Certificate is revoked for any reason, the Registration Authority that processed the Subscriber's Entrust SSL Web Server 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 SSL Web Server Certificate Application. Revocation of an Entrust SSL Web Server Certificate shall not affect any of the Subscriber's contractual obligations under this Entrust SSL Web Server Certification Practice Statement, the Subscriber's Subscription Agreement, or any Relying Party Agreements.

4.4.2 Who Can Request Revocation

A Subscriber may request revocation of their Entrust SSL Web Server Certificate at any time for any reason. If a Subscriber requests revocation of their Entrust SSL Web Server Certificate, the Subscriber must be able to validate themselves as set forth in Section 3.4 to the Registration Authority that processed the Subscriber's Entrust SSL Web Server Certificate Application. The Entrust SSL Web Server Certification Authorities shall not be required to revoke and the Registration Authorities operating under the Entrust SSL Web Server Certification Authorities shall not be required to request revocation of an Entrust SSL Web Server Certificate until a Subscriber can properly validate themselves as set forth in Section 3.4 and 4.4.3. An Entrust SSL Web Server Certification Authority shall be entitled to revoke and shall revoke, and a Registration Authority operating under an Entrust SSL Web Server Certification Authority shall be entitled to request revocation of and shall request revocation of, a Subscriber's Entrust SSL Web Server Certificate at any time for any of the reasons set forth in Section 4.4.1.

4.4.3 Procedure for Revocation Request

A Registration Authority operating under an Entrust SSL Web Server Certification Authority shall authenticate a request by a Subscriber for revocation of their Entrust SSL Web Server Certificate by requiring (i) some subset of the information provided by the Subscriber with the Subscriber's Entrust SSL Web Server Certificate Application, or (ii) the pass phrase submitted by the Subscriber with the Subscriber's Entrust SSL Web Server Certificate Application or 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 SSL Web Server Certification Authority that issued such Entrust SSL Web Server Certificate. The Entrust SSL Web Server Certification Authority receiving such revocation request shall immediately acknowledge the revocation request via email and initiate an investigation into the circumstances and criticality of the request. The Entrust SSL Web Server Certification Authority shall make all reasonable efforts to post the serial number of the revoked Entrust SSL Web Server Certificate to a CRL in an Entrust Repository within one (1) business day of receiving such revocation request. If a Subscriber's Entrust SSL Web Server Certificate is revoked for any reason, the Registration Authority that requested revocation of the Subscriber's Entrust SSL Web Server Certificate shall make a commercially reasonable effort to notify the Subscriber by sending an email to the technical and security contacts specified in the Subscriber's Entrust SSL Web 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 SSL Web Server 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 SSL Web Server Certification Authorities do not suspend Entrust SSL Web Server Certificates.

4.4.6 Who Can Request Suspension

Entrust SSL Web Server Certification Authorities do not suspend Entrust SSL Web Server Certificates.

4.4.7 Procedure for Suspension Request

Entrust SSL Web Server Certification Authorities do not suspend Entrust SSL Web Server Certificates.

4.4.8 Limits on Suspension Period

Entrust SSL Web Server Certification Authorities do not suspend Entrust SSL Web Server Certificates.

4.4.9 CRL Issuance Frequency

Entrust SSL Web Server Certification Authorities shall use commercially reasonable efforts to issue CRLs at least once every twenty-four (24) hours with a validity period of no greater than ten (10) days. CRLs will generally be issued at approximately 12.00 a.m. In certain circumstances, CRLs may also be issued between these intervals, such as in the event of the detection of a serious Compromise.

4.4.10 CRL Checking Requirements

A Relying Party shall check whether the Entrust SSL Web Server Certificate that the Relying Party wishes to rely on has been revoked. A Relying Party shall check the Certificate Revocation Lists maintained in the appropriate Repository or perform an on-line revocation status check using OCSP to determine whether the Entrust SSL Web Server Certificate that the Relying Party wishes to rely on has been revoked. In no event shall Entrust or any independent third-party Registration Authorities operating under an Entrust SSL Web Server Certification Authority, 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 SSL Web Server Certificate, or (ii) any reliance by a Relying Party on an Entrust SSL Web Server 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 On-line Certificate Status Protocol (OCSP). Entrust SSL Web Server Certification Authorities shall use commercially reasonable efforts to update OCSP responses at least once every twenty-four (24) hours with a validity period of seven (7) days. The location of the OCSP response is included in the Entrust SSL Web Server Certificate to support software applications that perform automatic certificate status checking. A Relying Party can also be check certificate revocation status directly with the Repository at www.entrust.net.

4.4.12 On-line Revocation Checking Requirements

Refer to Section 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 SSL Web Server Certificate has been Compromised, the Subscriber shall immediately notify the Registration Authority that processed the Subscriber's Entrust SSL Web Server Certificate Application, using the procedures set forth in Section 4.4.3, of such suspected or actual Compromise. The Subscriber shall immediately stop using such Entrust SSL Web Server Certificate and shall remove such Entrust SSL Web Server Certificate from any devices and/or software in which such Entrust SSL Web Server Certificate has been installed. The Subscriber shall be responsible for investigating the

circumstances of such Compromise or suspected Compromise and for notifying any Relying Parties that may have been affected by such Compromise or suspected Compromise.

4.5 Security Audit Procedures

Significant security events in the Entrust SSL Web Server Certification Authorities are automatically time-stamped and recorded as audit logs in audit trail files. The audit trail files are processed (reviewed for policy violations or other significant events) on a regular basis. Authentication codes are used in conjunction with the audit trail files to protect against modification of audit logs. Audit trail files are archived periodically. All files including the latest audit trail file are moved to backup media and stored in a secure archive facility.

The Entrust SSL Web Server Certification Authorities and all Registration Authorities operating under an Entrust SSL Web Server Certification Authority record in detail every action taken to process an SSL Web Server Certificate Request and to issue a SSL Web Server Certificate, including all information generated or received in connection with a SSL Web Server 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 SSL Web Server 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 SSL Web Server Certification Authority and Subscriber SSL Web Server Certificate lifecycle management events, including:
   a. SSL Web Server 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 SSL Web Server Certificate Requests;
   e. Issuance of SSL Web Server Certificates; and
   f. Generation of Certificate Revocation Lists (CRLs) and OCSP messages.

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

4.6 Records Archival

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

Entrust SSL Web Server Certification Authority system. Backup files are stored at a secure and separate geographic location.

4.7 Key Changeover

Subscribers are issued Entrust SSL Web Server Certificates that expire after a defined period of time to minimize the exposure of the associated Key Pair. For this reason, a new Key Pair must be created and that new Public Key must be submitted with each Entrust SSL Web Server Certificate Application to replace an expiring Entrust SSL Web Server Certificate. The process for renewing an Entrust SSL Web Server Certificate is described in Section 3.2.

4.8 Compromise and Disaster Recovery

Entrust SSL Web Server Certification Authorities have a disaster recovery plan to provide for timely recovery of services in the event of a system outage.

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

4.9 CA Termination

In the event that an Entrust SSL Web Server Certification Authority ceases operation, all Entrust SSL Web Server Certificates issued by such Entrust SSL Web Server Certification Authority shall be revoked.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Controls

Entrust/Authority™ software is used as the software component of the Entrust SSL Web Server Certification Authorities. The hardware and software for an Entrust SSL Web Server Certification Authority is located in a secure facility with physical security and access control procedures that meet or exceed industry standards. The room containing the Entrust/Authority software is designated a two (2) person zone, and controls are used to prevent a person from being in the room alone. Alarm systems are used to notify security personnel of any violation of the rules for access to an Entrust SSL Web Server Certification Authority.

5.2 Procedural Controls

An Entrust SSL Web Server Certification Authority has a number of trusted roles for sensitive operations of the Entrust SSL Web Server Certification Authority software. To gain access to the Entrust/Authority software used in an Entrust SSL Web Server Certification Authority, operational personnel must undergo background investigations. Entrust SSL Web Server Certification Authority operations related to adding administrative personnel or changing Certification Authority policy settings require more than one (1) person to perform the operation.

5.3 Personnel Controls

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

The signing Key Pair for an Entrust SSL Web Server Certification Authority is created during the initial start up of the Entrust/Master Control application and is protected by the master key for such Entrust SSL Web Server Certification Authority. Hardware key generation is used which is compliant to at least FIPS 140-1 level 3.

6.1.2 Private Key Delivery to Entity

Not applicable.

6.1.3 Public Key Delivery to Certificate Issuer

The Public Key to be included in an Entrust SSL Web Server Certificate is delivered to Entrust SSL Web Server Certification Authorities in a Certificate Signing Request (CSR) as part of the Entrust SSL Web Server Certificate Application process.

6.1.4 CA Public Key Delivery to Users

The Public-Key Certificate for Entrust SSL Web Server Certification Authorities is cross certified by the Entrust Root Certification Authority. The self-signed Public-Key Certificate for the Entrust Root Certification Authority is pre-installed in common World Wide Web browser and web server software by the applicable software manufacturers.

6.1.5 Key Sizes

The SSL server key sizes are determined by the Subscriber's cryptographic module.

6.1.6 Public-Key Parameters Generation

The Subscriber's World Wide Web server software controls which Public-Key parameters are used.

6.1.7 Parameter Quality Checking

The quality of the Public-Key parameters is governed by the Subscriber's World Wide Web server software that generates the parameters. Neither Entrust nor any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, nor any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing make any representations or provide any representations, warranties or conditions whatsoever about the quality of the Public Key contained in an Entrust SSL Web Server Certificate.

6.1.8 Hardware/Software Key Generation

The method for generating the Subscriber's Key Pair associated with an Entrust SSL Web Server Certificate is solely under the control of the Subscriber, and neither Entrust nor any independent third-party Registration Authority operating under an Entrust SSL Web Server Certification Authority, nor any Resellers or Co-marketers, or any subcontractors, distributors, agents, suppliers, employees, or directors of any of the foregoing shall have any responsibility or liability whatsoever for the generation of the Subscriber's Key Pair.

6.1.9 Key Usage Purposes

Entrust SSL Web Server Certificates issued by an Entrust SSL Web Server Certification Authority contain the keyUsage and the extendkeyUsage Certificate extensions restricting the purpose for which an Entrust SSL Web Server Certificate can be used. Subscribers and Relying Parties shall only use Entrust SSL Web

Server Certificates in compliance with this Entrust SSL Web Server Certification Practice Statement and applicable laws.

6.2 Private Key Protection

The Entrust SSL Web Server Certification Authorities use Entrust/Authority software in conjunction with hardware certified to FIPS 140 level 3 to protect the Entrust SSL Web Server Certification Authorities' Private Keys. Subscribers are responsible for protecting the Private Key associated with the Public Key in the Subscriber's Entrust SSL Web Server Certificate. Entrust does not escrow the Entrust SSL Web Server Certification Authorities' Private Keys.

6.3 Other Aspects of Key Pair Management

Entrust SSL Web Server Certificates contain a validity period. The Key Pair associated with the Entrust SSL Web Server Certificate is expired at the time of the certificate expiry or at the time of re-key, whichever occurs first. Key Pairs associated with Entrust SSL Web Server Certificates are not renewed.

6.4 Activation Data

No stipulation.

6.5 Computer Security Controls

The workstations on which the Entrust SSL Web Server Certification Authorities operate are physically secured as described in Section 5.1 The operating systems on the workstations on which the Entrust SSL Web Server Certification Authorities operate enforce identification and authentication of users. Access to Entrust/Authority software databases and audit trails is restricted as described in this Entrust SSL Web Server Certification Practice Statement. All operational personnel that are authorized to have access to the Entrust SSL Web Server 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 SSL Web Server Certification Authorities.

6.6 Life Cycle Technical Controls

The efficacy and appropriateness of the security settings described in this Entrust SSL Web Server Certification Practice Statement are reviewed on a yearly basis. A risk and threat assessment will be performed to determine if key lengths need to be increased or operational procedures modified from time to time to maintain system security.

6.7 Network Security Controls

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

6.8 Cryptographic Module Engineering Controls

The Entrust SSL Web Server Certification Authority application software cryptographic module is designed to conform to FIPS 140 level 2 requirements. Optional hardware tokens may be used to generate Key Pairs that may conform with higher levels of FIPS validation, but which must at least conform to level 2.

7 Certificate and CRL Profiles

The profile for the Entrust SSL Web Server Certificates and Certificate Revocation List (CRL) issued by an Entrust SSL Web Server 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 Certificate Profile

The following X.509 version 3 Certificate format is used by the Entrust SSL Web Server Certification Authorities:

1. Version: set to v3
2. Extensions: as stipulated in IETF RFC 3280
3. Algorithm object identifiers: as specified in IETF RFC 3279 Algorithms and Identifiers for the Internet X.509 PKI Certificate and Certificate Revocation List (CRL) Profile
4. Name forms: as stipulated in Section 3.1.1
5. Name constraints are not used
6. Certificate Policy OID: **1.2.840.113533.7.75.2**
7. Policy constraints are not used
8. Policy qualifiers:
   - CPSUri: http://www.entrust.net/CPS
   - userNotice: **The Entrust SSL Web Server Certification Practice Statement (CPS) 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. Copyright (c) 2002 Entrust Limited**
9. Certificate policies extension is marked Not Critical

7.2 CRL Profile

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

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

7.3 OCSP Profile

The profile for the Entrust SSL Online Certificate Status Protocol (OCSP) messages issued by an Entrust SSL Web Server 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 the Entrust SSL Web Server Certification Practice Statement and the terms and conditions contained herein from time to time. Modifications to the Entrust SSL Web Server Certification Practice Statement that, in the judgment of Entrust, will have little or no impact on Applicants, Subscribers, and Relying Parties, may be made with no change to the Entrust SSL Web Server Certification Practice Statement version number and no notification to Applicants, Subscribers, and Relying Parties. Such changes shall become effective immediately upon publication in the Entrust Repository.

Modifications to the Entrust SSL Web Server Certification Practice Statement that, in the judgment of Entrust may have a significant impact on 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 Entrust SSL Web Server Certification Practice Statement prior to such effective date. In the event that Entrust makes a significant modification to Entrust SSL Web Server Certification Practice Statement, the version number of the Entrust SSL Web Server Certification Practice Statement shall be updated accordingly. Unless a Subscriber ceases to use, removes, and requests revocation of such Subscriber's Entrust SSL Web Server Certificate(s) prior to the date on which an updated version of the Entrust SSL Web Server Certification Practice Statement becomes effective, such Subscriber shall be deemed to have consented to the terms and conditions of such updated version of the Entrust SSL Web Server Certification Practice Statement and shall be bound by the terms and conditions of such updated version of the Entrust SSL Web Server Certification Practice Statement.

8.2 Publication and Notification Policies

Prior to major changes to this Entrust SSL Web Server Certification Practice Statement, notification of the upcoming changes will be posted in the Entrust Repository.

8.3 CPS Approval Procedures

This Entrust SSL Web Server Certification Practice Statement and any subsequent changes shall be approved by the Entrust Policy Authority.

9 Acronyms

CA	Certification Authority
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

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

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 an Entrust SSL Web Server Certification Authority the right to promote Entrust SSL Web Server Certificates.

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

CPS: see Certification Practice Statement.

CRL: see Certificate Revocation List.

Cross Certificate(s): shall mean a Certificate(s) that (i) includes the public key of a public-private key pair generated by an Entrust SSL Web Server Certification Authority; and (ii) includes the digital signature of an Entrust Root Certification Authority.

Entrust: means Entrust Limited.

Entrust.net: means Entrust Limited.

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

Entrust Repository: means a collection of databases and web sites that contain information about Entrust SSL Web Server Certificates and services provided by Entrust in respect to Entrust SSL Web Server Certificates, including among other things, the types of Entrust SSL Web Server Certificates issued by the Entrust SSL Web Server Certification Authorities, the services provided by Entrust in respect to Entrust

SSL Web Server Certificates, the fees charged by Entrust for Entrust SSL Web Server Certificates and for the services provided by Entrust in respect to Entrust SSL Web Server Certificates, Certificate Revocation Lists, the Entrust SSL Web Server Certification Practice Statement, and other information and agreements that are intended to govern the use of Entrust SSL Web Server Certificates.

Entrust SSL Web Server 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 SSL Web Server Certificates.

Entrust SSL Web Server Certification Practice Statement: means this document.

Entrust SSL Web Server CPS: See Entrust SSL Web Server Certification Practice Statement.

Entrust SSL Web Server Certificate: means an SSL Certificate issued by an Entrust SSL Web Server Certification Authority for use on World Wide Web servers.

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

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

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

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

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

OID: see Object Identifier.

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

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

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

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

RA: see Registration Authority.

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

Server Certification Authority generate, digitally sign, and issue a Entrust SSL Web Server Certificate containing the information verified by the Registration Authority.

Relying Party: means a person, entity, or organization that relies on or uses an Entrust SSL Web Server Certificate and/or any other information provided in a Repository under an Entrust SSL Web Server 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 independent third-party Registration Authority or Reseller under an Entrust SSL Web Server Certification Authority in respect to the provision and use of certain information and services in respect to Entrust SSL Web Server Certificates.

Repository: means a collection of databases and web sites that contain information about Certificates issued by a Certification Authority including among other things, the types of Certificates and services provided by the Certification Authority, fees for the Certificates and services provided by the Certification Authority, Certificate Revocation Lists, descriptions of the practices and procedures of the Certification Authority, and other information and agreements that are intended to govern the use of Certificates issued by the Certification Authority.

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

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

