Trustwave

Certification Practices Statement

Version 2.0.1

Effective Date: July 31, 2008

Trustwave

Certification Practices Statement

Published date: July 31, 2008

Trademark Notices

Requests for any other permission to reproduce this Certification Practices Statement and the associated Certificate Policies (as well as requests for copies) shall be addressed to:

Trustwave
Attn: Legal Department
70 W. Madison Street, Suite 1050
Chicago, IL 60602
USA

Requests can also be made via email to ca@trustwave.com.

Corporate History

On June 1, 2007, Trustwave Holdings, Inc. acquired XRamp Security Services, Inc., successor to SecureTrust Corporation.

Table of Contents

Revision History

Changes	Approving Manager	Date
Ver. 2.0.0 - Initial Publication	Certification Practice Board "CPB"	07 MAY 08
Ver. 2.0.1 – Sections 1.1, 3.1, 3.2, 4.2, 6.3, 7.1.2.5 related to Code Signing	CPB	31 JULY 08

1. INTRODUCTION

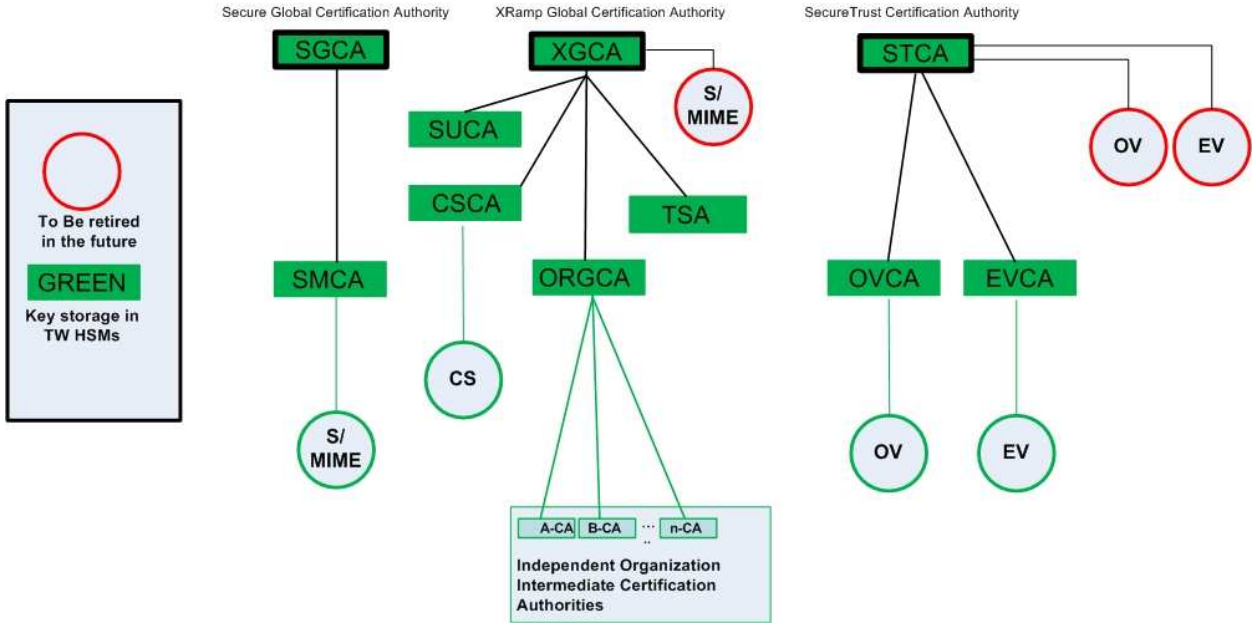
This document is the Trustwave Holdings, Inc. (hereinafter "Trustwave") Certification Practices Statement ("CPS") which details the following information:

- the practices, procedures, and infrastructure employed by the Trustwave Certification Authority ("CA") for its operations and business continuity,
- the practices and procedures employed in the creation, management, and termination of our Root CA Keys,
- the practices and procedures that apply generally to all End-Entity Certificates issued by our CA,
- the physical, environmental, and logical security controls employed by Trustwave to protect our Root CA Certificates, and
- the legal structure of the relationship between Trustwave, Subscribers (End-Entities), and Relying Parties.

Trustwave provides certification services for a number of different types of End-Entity Certificates, each of which may have differing uses and purposes which necessitate different processes and procedures employed during the vetting process and the overall Certificate lifecycle. The digital Certificate lifecycle includes public and private key generation, the vetting of the information contained within the Certificate by the CA, the CA signing of the Certificate, the implementation and use of the digital Certificate, and finally, the termination of use of the digital Certificate. The processes and procedures used for the different Certificate types are also detailed in the relevant sections within this document.

In summary, this CPS focuses on the overall CA operations and Root CA Key policies and procedures while also focusing on the policies and procedures surrounding End-Entity Certificates. This CPS constitutes the entirety of the obligations, representations, warranties, policies, and procedures that apply to a digital Certificate issued by Trustwave. In the event that there is a discrepancy between the following procedures and the CA/Browser Forum Guidelines, the CA/Browser Forum Guidelines will supersede the procedures detailed below.

1.1 Overview



Trustwave operates and maintains three separate Root CA Keys identified by the following names:

- **Secure Global Certification Authority** ("SGCA")
- **XRamp Global Certification Authority** ("XGCA")
- **SecureTrust Certification Authority** ("STCA")

This CPS governs the operation and maintenance of and is applicable to the above-listed Root CA Keys. In addition, Trustwave maintains six subordinate certification authorities and a time-stamping authority immediately subordinate to these three Root CA's as depicted in the diagram above:

- **Trustwave S/MIME Certification Authority** ("SMCA"). This CA only issues Certificates for S/MIME (e-mail) use.
- **Trustwave Special Use Certification Authority** ("SUCA"). This CA is reserved for future use.
- **Trustwave Organizational Certification Authority** ("ORGCA"). This CA is reserved for future use.
- **Trustwave Time stamping Authority** ("TSA"). This capability responds only to time stamping requests.
- **Trustwave Code signing Certification Authority** ("CSCA"). This CA issues Certificates for code signing use.
- **Trustwave Organizationally Validated Certification Authority** ("OVCA"). This CA issues OV Certificates for server (e.g. WWW server) implementations.
- **Trustwave Extended Validation Certification Authority** ("EVCA"). This CA issues EV Certificates for server (e.g. WWW server) implementations.

The nine certification authorities and the Trustwave Time Stamping Authority are collectively known as the "Trustwave Public Key Infrastructure Hierarchy" ("TPH"). All activities of the TPH

listed above, and the Certificate policies associated with the Certificates that these CA's issue, are defined and governed by this document.

In addition, the ORGCA as depicted in the diagram above, the practices associated with this certification authority, and of Certificates issued to other organizations by the ORGCA are not delimited within this document, however, the governance and requirements for all subordinate certification authorities underneath ORGCA are defined and contained herein.

Trustwave issues the following Certificate types, which can be identified by the Certificate Policy Object Identifier ("OID" or "CP OID") contained within the End-Entity Certificate:

- Extended Validation ("EV") SSL Certificates
  CP OID ([†]): 2.16.840.1.114404.1.1.2.4.1
  CP OID (future): 1.3.6.1.4.1.30360.3.3.3.3.4.3.3

- Organization Validation ("OV") SSL Certificates
  CP OID: 2.16.840.1.114404.2.1.2
  CP OID (future): 1.3.6.1.4.1.30360.3.3.3.3.4.4.3

- Domain Validation ("DV") SSL Certificates
  CP OID (prior to 05/07/2008): 2.16.840.1.114404.2.1.1
  Note: Trustwave no longer issues DV certificates.

- Email S/MIME Certificates
  CP OID: 2.16.840.1.114404.2.2.1
  CP OID (future): 1.3.6.1.4.1.30360.3.3.3.5.4.3.3

- Extended Validation ("EV") Code Signing Certificates
  CP OID (prior to 05/07/2008): 2.16.840.1.114404.2.4.1
  CP OID: 1.3.6.1.4.1.30360.3.3.3.4.4.3.3

- Organization Validation ("OV") Code Signing Certificates
  CP OID: 1.3.6.1.4.1.30360.3.3.3.4.4.3.4

All Certificates issued by Trustwave will contain a CP OID so that End-Entities and Relying Parties can identify the type of Certificate and the policies and procedures that were followed in the during the Certificate lifecycle including the vetting processes used prior to the issuance and the intended purposes of the Certificate.

All of the CP's are contained within this CPS, which can be found at https://ssl.trustwave.com/CA.

[†] EV Certificates issued under this CPS will continue to use the deprecated CP OID until such time it can be established that EV functionality will perform properly with the new CP OID in effectively all web browser software, at which time we will switch to the new CP OID. EV Certificates with the deprecated CP OID with a Validity Period starting on or after May 7, 2008 will follow this CPS. For EV Certificates with a Validity Period starting prior to May 7, 2008, please refer to the "CPS for Extended Validation Certificates", Version 1.0.1, dated November 1st, 2006 located at https://ssl.trustwave.com/CA.

1.2 Document Name and Identification

This document is the Trustwave Certification Practices Statement. All Trustwave Certificates contain a CP OID corresponding to the applicable Certificate type (See Section 1.1). Because this CPS is incorporated within all CP's, this CPS does not have a unique OID associated with it. This CPS contains the relevant CP's.

1.3 PKI Participants

1.3.1 Certification Authorities

The only Certification Authority specifically governed by this document is Trustwave. External CA's who receive a Subordinate Root CA Certificate from Trustwave are governed by the applicable CP associated with that Certificate and/or any contracts that may be in place between Trustwave and the External CA. External CAs shall implement their own CPS that governs the operations of their CA.

1.3.2 Registration Authorities

A Registration Authority ("RA") is an entity that performs identification and authentication of Certificate applicants for end-user Certificates. An RA may vet subscribers, initiate or pass along Certificate requests, and approve or pass along other Certificate lifecycle actions including renewals, re-keys, and revocations. Trustwave may act as an RA for Certificates it issues.

Trustwave may enter into agreements with third parties to operate as an RA under this CPS. Third party RA's shall contractually agree to the terms of this CPS, the relevant CP's, and the terms of their enterprise services agreement with Trustwave. RA's may, in their discretion, proscribe more restrictive practices.

The most common reason that Trustwave contracts with a third party to be an RA is in order to service foreign markets. A business entity that is located in a foreign market and serves as an RA for Trustwave may be able to more easily service the requirements of this CPS and the associated CP's due to their knowledge of the local laws, business customs, and language.

1.3.3 Subscribers

Subscribers are the end entities that hold Certificates issued by Trustwave. A Subscriber can be an individual, an organization, a corporation, or any other type of legal entity. Subscribers are sometimes also referred to as Applicants prior to the issuance of a Certificate. The context in which either term is used will invoke the correct understanding.

1.3.4 Relying Parties

A Relying Party is any individual or entity that relies on the information contained within a Certificate issued by Trustwave to perform an act. An example of such an act would be an individual who relies upon the information contained within a Certificate when making a connection to a secure web site to confirm that the website owner is, in fact, who he, she, or it claims to be. A Relying Party may also be a Subscriber.

1.3.5 Other Participants

The three main participants in a PKI are the CA, Subscribers, and Relying Parties. However, a device can also have a Certificate associated with it that is not connected to a specific entity or individual. In cases where a device, such as a firewall, a router, or a server has a Certificate, the Relying Party should refer to the appropriate Certificate Policy embedded in that specific Certificate to determine the purpose, usefulness, and policies that apply.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

Trustwave issues several different types of Certificates, which are all intended for different purposes. Please refer to the CP identified by the CP OID embedded within the Certificate to determine the appropriate uses of the particular Certificate in question.

1.4.2 Prohibited Certificate Uses

Certificates issued by Trustwave shall be used only to the extent that the use is consistent with applicable law, including without limitation, applicable export or import laws.

Trustwave Certificates are not designed, intended, or authorized for use or resale as control equipment in hazardous circumstances or for uses requiring fail-safe performance such as the operation of nuclear facilities, aircraft navigation or communication systems, or weapon control systems, where failure could lead directly to death, personal injury, or severe environmental damage.

Trustwave issues several different types of Certificates, each of which have varied intended uses and purposes. Please refer to the CP identified by the CP OID embedded within the Certificate for further information regarding uses of Certificates prohibited by that particular Certificate type. Certificates may only be used for the purpose specifically stated in the applicable CP.

Trustwave occasionally re-keys Intermediate CAs, and Subscribers may re-key their Certificates upon their request. Third party applications or platforms may not operate as designed or intended after a re-key. It is the sole obligation of the Subscriber to make any modifications necessary and/or perform any required testing to assure a Certificate will continue to work as intended upon a re-key. Trustwave does not warrant any use of Intermediate CAs as root Certificates. If Trustwave determines that it is necessary or appropriate to re-key an Intermediate CA, notice to do so will be provided to Subscribers at least 30 days in advance of a re-key occurring. Upon a re-key event, Subscribers must cease reliance upon the old keys. Trustwave shall not warrant any actions or activities by Subscribers based upon the previous keys following a re-key event of a CA.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Trustwave Holdings, Inc.
70 West Madison Street, Suite 1050
Chicago, Illinois 60602

USA

1.5.2 Contact Persons

Trustwave CA Operational Committee
Attn: Andrew Gray & Annabel Lewis
70 West Madison Street, Suite 1050
Chicago, Illinois 60602
USA

1.5.3 Person Determining CPS and CP Suitability for the Policy

Trustwave's Certification Practice Board ("CPB"), reports to the Trustwave Holdings, Inc.'s Board of Directors, which determines the suitability and applicability of this CPS and all related CP's. The members of the CPB, as well as their tenure, are determined by the Board of Directors of Trustwave. As of March 31, 2008, the following individuals comprise the CPB:

- General Counsel – Mr. Phillip Smith
- Chief Operating Officer – Mr. Andrew Bokor
- Chief Technology Officer – Mr. Larry Podmolik

1.5.4 CPS and CP Approval Procedures

All changes and revisions to this CPS and the related CP's shall be approved by the CPB. All amendments and updates shall be posted in Trustwave's repository located at https://ssl.trustwave.com/CA.

1.6 Definitions and Acronyms

Activation Data: Data (other than keys) required for operating hardware or software cryptographic modules. Examples include personal identification numbers (PINs), passwords, and pass phrases.

Authentication: The process of establishing identity based on the possession of a trusted credential.

Certificate: A public key certificate.

Certificate Approver: A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve Certificate Requests submitted by other Certificate Requesters.

Certification Authority: An entity which issues, manages, revokes, and renews Certificates.

Certificate Policy (CP): A "named set of rules that indicates the applicability of a Certificate to a particular community and/or class of application with common security requirements" [X509].

Certification Practices Statement (CPS): A statement of the practices which a Certification Authority employs in issuing and managing Certificates.

Certificate Revocation List (CRL): A list of Certificates previously issued by the subject CA that have been subsequently compromised or otherwise invalidated.

Compromise: Suspected or actual unauthorized disclosure, loss, loss of control or use of a Private Key associated with Certificate.

Contract Signer: A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements and other related agreements.

Cross-Certificate: A Certificate issued by the subject CA certifying the public key of another CA.

Data Integrity: Cryptographically secure assurance that no change has occurred in a document, message, data file, or data transmission.

Decryption Private Key: A private key used to decrypt data or session keys encrypted by the corresponding public key. In the context of this document, the public key is presumed to be contained and conveyed by an encryption Certificate.

Distinguished Name: A distinguished name is the concatenation of selected attributes from each entry, called the *relative distinguished name* (RDN), in the X.500 directory tree along a path leading from the root of the X.500 namespace down to the named entry.

FMS Community: The US Department of Treasury, Financial Management Service (FMS), or any person or organization operating under the authority and direction of the FMS, either directly or through a contractual relationship.

Domain (of a CA): The scope of authority of a CA, generally limited to RA's and End-Entities registered with or certified by the CA.

Encryption Certificate: A Certificate containing and conveying a public key used to encrypt electronic messages, files, documents, data transmissions, etc., or to establish a session key for those purposes.

End-Entity (EE): A person, computer system, or a communications device that is a subject or user of a Certificate, but is not a CA or RA. An End-Entity is a Subscriber, a Relying Party, or both.

Entity: A CA, RA, or End-Entity.

Identity Certificate: A Certificate issued for the purpose of binding the identity of the subject (as stated in the Certificate) to a public key issued to that subject. In X.509 Certificates, the identity of the subject is equivalent to the Distinguished Name of the subject.

Intersite Trust Agreement: An agreement between sites for allowing cross-site use of Certificates.

Key: A value supplied to a cryptographic algorithm to encrypt or decrypt data.

Key Materials: A tangible representation of a key. Examples include a key stored in computer memory, computer disk, smart card, or other key carrier.

PKI: See Public Key Infrastructure.

Place of Business: An entity's principal place of business, a satellite office, or a regional office.

Private Key: The portion of a public-private key pair known only to the holder.

Public Key: The portion of a public-private key pair that may be publicly known or distributed without reducing the security of the cryptography system. In the context of this Policy, Public Keys (after initial issuance) are always distributed through the use of Public Key Certificates.

Public Key Algorithm: A cryptographic algorithm in which the encryption and decryption functions are divided between a pair of mathematically related keys. In some common Public Key Algorithms (e.g., RSA), the encryption/decryption functions are reciprocal, i.e., either key of the pair can be used to encrypt or decrypt, with the other key able to decrypt or encrypt respectively.

Public Key Certificate: The public key portion of a public-private key pair that has been digitally signed by a CA, thereby certifying the validity and data integrity of the Public Key contained in the Certificate, in accordance with the applicable Certificate Policy.

Public Key Infrastructure (PKI): A system for using public key cryptography and providing a trusted mechanism for distributing and managing public keys through the appropriate use of Certificates.

Qualified Government Agency Source: A regularly-updated and current online publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are maintained by a government entity.

Qualified Government Information Source ("QGIS"): A regularly updated and current publicly available source which is designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided they are maintained by a government entity.

Qualified Government Tax Information Source ("QGTIS"): A QGIS that specifically contains tax information, e.g. the I.R.S. in the United States.

Qualified Independent Information Source ("QIIS"): A regularly-updated and current publicly available database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information. A commercial database is a QIIS if the following are true: (i) data it contains that will be relied upon has been independently verified by other independent information sources; (ii) the database distinguishes between self-reported data and data reported by independent information sources; (iii) the database provider identifies how frequently they update the information in their database; (iv) changes in the data that will be relied upon will be reflected in the database in no more than twelve (12) months; and (v) the database

provider uses authoritative sources independent of the subject, or multiple corroborated sources, to which the data pertains.

Registration Authority (RA): A person or other entity operating under the authority of a CA that is responsible for identification and authentication of Certificate subjects and other duties as assigned in the site CPS.

Registration Number. The unique number or code assigned to an entity after its application for registration to do business in a particular jurisdiction is approved.

Registered Office. An entity's physical address identified in its application for registration to do business in a particular jurisdiction or its principal place of business.

Relying Party: Any user or recipient of a Certificate that acts in reliance on that Certificate. In this document, the terms "Certificate user" and "Relying Party" are used interchangeably.

SecureTrust: SecureTrust Corporation merged into XRamp Security which is a wholly-owned subsidiary of Trustwave Holdings, Inc., a Delaware corporation.

Session Key: A key, typically for a symmetric algorithm, established between communicating parties for subsequent encryption/decryption of electronic messages, files, documents, data transmissions, etc. Its use is generally limited to that purpose and a single transaction or session.

Signing Private Key: A private key used to create digital signatures.

Sponsor: A person or organization with which the Subscriber is affiliated (e.g., as an employee, user of service, or customer).

Subject End-Entity: An End-Entity that is the subject of a Certificate.

Subscriber: A person or entity who is the subject named or identified in a Certificate issued to such person or entity, holds a Private Key that corresponds to a Public Key listed in that Certificate, and the person or entity to whom digitally signed messages verified by reference to such Certificate are to be attributed.

Suspect Code: Code that contains malicious functionality or serious vulnerabilities, including spyware, malware, and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes.

Symmetric Algorithm: A cryptographic algorithm in which data is encrypted and decrypted using the same key.

Validity Period. A Certificate's period of validity. It typically begins 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 unless the Certificate is revoked before its expiration.

Verified Accountant Letter: A letter signed by a duly licensed accountant, with active status, whereby the accountant attests to the existence, validity and accuracy of the entity's legal

existence, name and/or assumed names under which Applicant conducts business and that such is current and duly registered in the appropriate jurisdiction.

Verified Legal Opinion: A letter signed by an attorney, with active status, licensed to practice law in the country of Applicant's jurisdiction of incorporation or registration or any jurisdiction where Applicant maintains an office or physical facility whereby the attorney attests to the existence, validity and accuracy of the entity's legal existence, name and/or assumed names under which Applicant conducts business and that such is current and duly registered in the appropriate jurisdiction.

ABBREVIATIONS

CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practices Statement
CRL	Certificate Revocation List
FQDN	Fully Qualified Domain Name
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
IEC	International Electro-technical Commission
IETF	Internet Engineering Task Force
IP	Internet Protocol
ISO	International Organization for Standardization
ITU	International Telecommunications Union
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PKIX	Public Key Infrastructure - X.509 (IETF Working Group)
RA	Registration Authority
RFC	Request for Comments
RSA	Rivest-Shamir-Adelman Encryption Algorithm
TPH	Trustwave Public-Key Hierarchy
TW	Trustwave

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

Trustwave maintains three separate Repositories:

(a) Certificate Repository. Digital Certificates that are issued to End-Entities are stored on a non-public file system and in an internal LDAP directory.

(b) Document Repository. Legal documents, including this CPS, associated CP's, Subscriber Agreements, Relying Party Agreements, and other documents related to our Digital Certificate services are publicly available on our web site at the following URL: https://ssl.trustwave.com/CA.

(c) Certificate Status Information Repository. Certificate status information is available through a publicly published Certificate Revocation List ("CRL") and/or

other online Certificate status protocols. Every Certificate issued from any of the Root CA Certificates governed by this CPS will contain information within the Certificate that will identify the location where Certificate status information can be found.

2.2 Publication of Certificate Information

Trustwave will maintain and publish a current version of this CPS, including its associated CP's, Subscriber Agreements, Relying Party Agreements, and all other relevant legal documents at the following URL: https://ssl.trustwave.com/CA. The repositories allow Relying Parties and others to view Certificate status information, including without limitation, a Certificate's revocation status.

Certificate status information is provided in accordance with the CP identified in each End-Entity Certificate.

2.3 Time or Frequency of Publication

Updates to this CPS and the associated CP's are approved and published as set forth in Section 9.12 herein. Subscriber Agreements and Relying Party Agreements are published as necessary. Certificates are published when issued. Certificate status information is published in accordance with the CP identified in each End-Entity Certificate. CRL information shall be generated and published on a daily basis.

2.4 Access Controls on Repositories

Information published in our Document Repository and Certificate Status Information Repository is available on a read-only basis. Information contained in our Certificate Repository is available to the End-Entity who owns the Certificate as well as Trustwave staff. Trustwave has physical and logical security controls in place to prevent unauthorized persons from adding, deleting, or modifying the information contained within its repositories.

3. IDENTIFICATION AND AUTHENTICATION

In the event that there is a discrepancy between the following procedures and the CA/Browser Forum Guidelines, the CA/Browser Forum Guidelines will supersede the procedures detailed below.

3.1 Naming

3.1.1 Types of Names

All Certificates issued by Trustwave certification authorities shall be in the form of and will comply with the ISO/ITU X.500 naming convention. All Certificates will have the subject field (subject alternative name) of the Distinguished Name set as per the following:

EV Certificates	In addition to the fully authenticated DNS name of the server, the common name component of the subject in extended validation Certificates shall include the following authenticated attributes as required by CA/Browser Forum Guidelines: 1. Organization name (OID 2.5.4.10)

	2. Domain name (OID 2.5.4.3) 3. Business category (OID 2.5.4.15) 4. Jurisdiction of Incorporation or Registration including: • Locality (OID 1.3.6.1.4.1.311.60.2.1.1) • State or province (OID 1.3.6.1.4.1.311.60.2.1.2) • Country (OID 1.3.6.1.4.1.311.60.2.1.3) Registration Number (OID 2.5.4.5) 5. Physical Address of Place of Business including: • Locality (OID 1.3.6.1.4.1.311.60.2.1.1) • State or province (OID 1.3.6.1.4.1.311.60.2.1.2) • Country (OID 1.3.6.1.4.1.311.60.2.1.3) 6. Registration Number (OID 2.5.4.5)
OV Certificates	The commonName (CN) component of the subject name in OV Certificates shall include the fully qualified DNS name of the service, which is usually that of the host supporting the service. The structure of a service's CN is designed to support SSL and TLS.
S/MIME Certificates	The Distinguished Name shall contain a generic string – "Trustwave SMIME user". The subject alternative name will be set to the authenticated Subscriber's e-mail address.
EV Code Signing Certificates	1. Organization name (OID 2.5.4.10) 2. Business category (OID 2.5.4.15) 3. Jurisdiction of Incorporation or Registration including: • Locality (OID 1.3.6.1.4.1.311.60.2.1.1) • State or province (OID 1.3.6.1.4.1.311.60.2.1.2) • Country (OID 1.3.6.1.4.1.311.60.2.1.3) Registration Number (OID 2.5.4.5) 4. Physical Address of Place of Business including: • Locality (OID 1.3.6.1.4.1.311.60.2.1.1) • State or province (OID 1.3.6.1.4.1.311.60.2.1.2) • Country (OID 1.3.6.1.4.1.311.60.2.1.3) 5. Registration Number (OID 2.5.4.5)
OV Code Signing Certificates	The commonName (CN) component of the subject name in OV Code Signing Certificates shall include the subject's full legal name.

3.1.2 Need for Names to be Meaningful

The subject field within the Certificates of the each of the TPH participants defined in section 1.1 shall uniquely identify each of the ten Trustwave capabilities in a human readable format. Additionally:

EV Certificates	Trustwave ensures via the practices and procedures as defined within this document, and in 3.2.2, that the subject name uniquely identifies the name of the EV Subscriber.
EV Code Signing Certificates	Trustwave ensures via the practices and procedures as defined within this document, and in 3.2.2, that the subject name uniquely identifies the name of the EV Code Signing Subscriber.
OV Certificates	All attributes of the subject shall be authenticated by Trustwave, to include a distinguished name, organization, and any

	organizational unit.
OV Code Signing Certificates	All attributes of the subject shall be authenticated by Trustwave to include a distinguished name, organization, and any organizational unit.
S/MIME Certificates	The distinguished name shall contain a generic string – "Trustwave SMIME user". The subject alternative name shall be unique for all SMIME Certificates issued

3.1.3 Anonymity or Pseudonymity of Subscribers

Anonymous or pseudonymous Certificates are not issued by Trustwave Certification Authorities, nor shall be issued to or by any subordinate CA within the organizational certification authority hierarchy.

3.1.4 Rules for Interpreting Various Name Forms

Name forms within Trustwave Certification Authority Certificates, Trustwave issued End-Entity Certificates, and any subordinate CA Certificate within the organizational certification authority hierarchy shall adhere to the ISO/ITU X.500 series naming standards.

3.1.5 Uniqueness of Names

The uniqueness of names within Trustwave issued digital Certificates shall be determined as per the following:

EV Certificates	The subject of all EV Certificates issued by Trustwave shall be unique. (Also see Appendix A)
EV Code Signing Certificates	The subject of all EV Code Signing Certificates issued by Trustwave shall be unique.
OV Certificates	The subject of all OV Certificates issued by Trustwave shall be unique.
OV Code Signing Certificates	The subject of all OV Code Signing Certificates issued by Trustwave shall be unique.
S/MIME Certificates	The subject of all SMIME digital Certificates shall be generic in the form of: "Trustwave SMIME user". The subject alternative name of all SMIME Certificates shall be unique.

3.1.6 Recognition, Authentication, and Role of Trademarks

Trustwave does not determine the validity or rights of a Subscriber or Applicant to use any name, trademarks, trade names, domain names, service marks, or other marks ("marks"). Applicants and Subscribers shall not use other parties' marks in their Certificate applications, Subscriber Agreement or other related documentation. Trustwave may, within its sole discretion, reject or suspend a Certificate application due to potential trademark infringement.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

All End-Entity applicants within the TPH shall submit a digitally signed PKCS#10 CSR to establish that it holds the private key corresponding to the public key to be included in a

Certificate. Trustwave shall verify that the CSR's signature was created by the private key associated with the public key in the CSR.

3.2.2 Authentication of Organization Identity

EV Certificates, Organizational CA Certificates	Trustwave will verify Applicant's legal existence, physical existence, operational existence, and domain control as shown below. A.) **<u>Legal Existence</u>** 1. Legal existence validation, as required by the CA/Browser Forum EV Guidelines, may be satisfied by performing each of the following: (a) Verification that Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the incorporating or registration agency in Applicant's jurisdiction of incorporation or registration, and not designated by labels such as "inactive", "invalid", "not current", or the equivalent; (b) Verification that the Applicant's formal legal name as recorded with the incorporating or registration agency in Applicant's jurisdiction of incorporation or registration matches Applicant's name on the EV Certificate request; (c) Obtain the specific registration number assigned to Applicant by the incorporating or registration agency in Applicant's jurisdiction of incorporation or registration. Where the incorporating or registration agency does not assign a registration number, Trustwave shall obtain Applicant's date of incorporation or registration; and (d) Obtain the identity and address of Applicant's registered agent or registered office (as applicable in Applicant's jurisdiction of incorporation or registration. 2. Verification of Applicant's Assumed Name a.) Verification Requirements. If, in addition to Applicant's formal legal name as recorded with the applicable incorporating agency or registration agency in Applicant's jurisdiction of incorporation or registration, Applicant's identity as asserted in its EV Certificate is to contain any assumed name (also known as "doing business as", "DBA" or "d/b/a" in the U.S., and "trading as" in the U.K.) under which applicant conducts business, Trustwave shall verify both of the following: 1. Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business; and 2. That such filing continues to be valid.

b.) Acceptable Method of Verification. To verify any assumed name under which Applicant conducts business:

1. Trustwave may verify the assumed name through use of a qualified government information source (as set forth by the CA/Browser Forum EV Guidelines) operated by, or on behalf of, an appropriate government agency in the jurisdiction of Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, web address, or telephone; or
2. Trustwave may verify the assumed name through use of a QIIS provided that the QIIS has verified the assumed name through the appropriate government agency; or
3. Trustwave may rely on a Verified Legal Opinion, or a Verified Accountant Letter that indicates the assumed name under which Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

B.) **Physical Existence**

Trustwave shall verify that the Applicant's physical existence and business presence by verifying that the physical address provided by Applicant is an address where Applicant conducts business operations (e.g., not a mail drop or P.O. box), and is the address of Applicant's Place of Business.

a.) Acceptable Methods of Verification. To verify the address of Applicant's Place of Business for Applicants whose Place of Business is in the same country as Applicant's jurisdiction of incorporation or registration:

i. For Applicants listed at the same Place of Business address in the current version of either at least one (1) QIIS or a Qualified Governmental Tax Information Source, Trustwave shall confirm that Applicant's address as listed in the EV Certificate Request is a valid business address for Applicant by reference to such QIIS or a Qualified Governmental Tax Information Source, and MAY rely on Applicant's representation that such address is its Place of Business.

ii. For Applicants who are not listed at the same Place of Business address in the current version of either at least one (1) Qualified Independent

	Information Source or a Qualified Governmental Tax Information Source, Trustwave shall confirm that the address provided by Applicant in the EV Certificate Request is in fact Applicant's business address, by obtaining documentation of a site visit to the business address which shall be performed by a reliable individual or firm. The documentation of the site visit shall: 1. Verify that Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.); 2. Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location; 3. Indicate whether there is a permanent sign (that cannot be moved) that identifies Applicant; 4. Indicate whether there is evidence that Applicant is conducting ongoing business activities at the site (e.g., that it is not just a mail drop, P.O. box, etc.); and 5. Include one or more photos of (i) the exterior of the site (showing signage indicating Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace. iii. For all Applicants, Trustwave may alternatively rely on a Verified Legal Opinion or a Verified Accountant Letter that indicates the address of Applicant's Place of Business and that business operations are conducted there. b.) For Applicants whose Place of Business is not in the same country as Applicant's Jurisdiction of Incorporation or Registration, Trustwave shall rely on a Verified Legal Opinion that indicates the address of Applicant's Place of Business and that business operations are conducted there. Additionally for both a.) and b.) above, the Applicant's telephone number shall also be verified by confirming Applicant's telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed; AND Trustwave shall also perform one of the following:

	i. Confirm that the telephone number provided by Applicant is listed as Applicant's or Parent/Subsidiary Company's telephone number for the verified address of its Place of Business in records provided by the applicable phone company, or alternatively, in either at least one (1) Qualified Independent Information Source or a Qualified Governmental Tax Information Source; OR ii. During a site visit, the person who is conducting the site visit shall confirm Applicant's or Parent/Subsidiary Company's main telephone number by calling it and obtaining an affirmative response sufficient to enable a reasonable person to conclude that Applicant is reachable by telephone at the number dialed. Trustwave shall also confirm that Applicant's main telephone number is not a mobile phone; OR iii. Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant's telephone number, as provided, is a main phone number for Applicant's Place of Business. C.) **Operational Existence** Trustwave shall verify that the Applicant's business operations have been in effect longer than 3 years or Applicant is listed in a current version of a QIIS. If neither of the above conditions are met, Trustwave shall perform one of the following: i. Verify Applicant has an active current Demand Deposit Account with a Regulated Financial Institution. Trustwave shall receive authenticated documentation directly from a Regulated Financial Institution verifying that Applicant has an active current Demand Deposit Account with the institution; OR ii. Rely on a Verified Legal Opinion or a Verified Accountant Letter to the effect that Applicant has an active current Demand Deposit Account with a Regulated Financial Institution D.) **Domain Name** Trustwave shall verify an Applicant's registration or that the Applicant has exclusive control over the domain name(s) to be listed in the Certificate by confirming that: a.) the domain is registered with Internet Corporation for Assigned Names and Numbers ("ICANN") –approved registrar

	or Internet Assigned Numbers Authority ("IANA")-approved registrar, b.) the WHOIS data should be public and should show the name, physical address, and administrative contact information for the organization. In cases where Applicant is not the registered holder of the domain name, Trustwave shall verify Applicant's exclusive right to use the domain names(s) by the following: a. In cases where the registered domain holder can be contacted using information obtained from WHOIS, or through the domain registrar, Trustwave shall obtain positive confirmation from the registered domain holder by paper mail, e-mail, telephone, or facsimile that Applicant has been granted the exclusive right to use the requested Fully Qualified Domain Name ("FQDN"); and b. Trustwave shall verify Applicant's exclusive right to use the domain name(s) using one of the following methods: 1. Relying on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name(s) in identifying itself on the Internet; or 2. Relying on a representation from the Contract Signer, or the Certificate approver, if expressly so authorized in a mutually-agreed upon contract. In cases where the registered domain holder cannot be contacted, Trustwave shall: a. Rely on a Verified Legal Opinion to the effect that Applicant has the exclusive right to use the specified domain name in identifying itself on the Internet; and b. Rely on a representation from the Contract Signer, or the Certificate approver, if expressly so authorized in a mutually-agreed upon contract, coupled with a practical demonstration by Applicant establishing that it controls the domain name by making an agreed-upon change in information found online on a web page identified by a uniform resource identifier containing Applicant's FQDN.
EV Code Signing Certificates	EV Code Signing Certificates shall be validated in the same manner as EV Certificates, except that domain name verification is not performed.
OV Certificates	The following validation procedures will be performed to validate

	the Subscriber's Certificate request: A.) **Organizational Validation** In order to manually validate the Subscriber's Organizational information, the Subscriber will be required to provide any one of the following documents to Trustwave that show reasonable proof that the organization is operating under the organizational name that is listed in their Certificate request: a. Organizational documents such as: Articles of Incorporation, Certificate of Incorporation, L.L.C., L.L.P., L.P., L.T.D., Fictitious Name, DBA, or any other standard documentation issued by or filed with the proper governmental authority. b. Third-party statements showing the use of the organizational name such as: Bank Statements and Merchant Account Statements. c. If the organization is a sole-proprietorship or the Certificate is being issued to an individual, then Trustwave will accept a copy of their driver's license, identity card, or passport. The above mentioned documents can be accepted via postal mail, facsimile, e-mail, delivery service, or hand delivery. In the event that none of the above information is readily available, Trustwave may consider other convincing factors which may be used to validate a Subscriber's Organizational information. B.) **Domain Name Verification** Due to the fact that many people do not put proper information in their WHOIS information, or domain names could be registered on the Subscriber's behalf by a third-party, Trustwave can validate Domain Name information by having a Trustwave employee or an authorized third-party contractor visit the website associated with the common name listed in the Certificate request to determine if the website that the common name resolves to appears to be in the control of the Subscriber. There are many ways in which this method can be used to validate the Subscriber's Domain Name information including, but not limited to the following: a. A Subscriber can post a special HTML Trustwave Validation page to their website which can then be visited by Trustwave to show that the Subscriber has control over the website. This validation page may be verified manually through a Trustwave employee visiting the page, or through automated processes. b. Any other means by which it can be reasonably established that Subscriber has control over the domain name listed in the Certificate request.

	The prime purpose for Domain Name validation is to establish that the Subscriber has control over the domain name listed in their Certificate request, or that they have authorization to purchase a SSL Certificate for the domain name listed in their Certificate request. C.) **Non-Standard Certificate Validation** In the event that Trustwave is unable to verify certain Applicant information for processing Certificate applications as described above, Trustwave may in its sole discretion issue the Certificate provided that Trustwave has taken, and documented, other reasonable steps to authenticate the Applicant and the issuance of such Certificate is authorized by a Trustwave manager.
OV Code Signing Certificates	OV Code Signing Certificates shall be validated in the same manner as OV Certificates, except that domain name verification is not performed.

3.2.3 Authentication of Individual Identity

S/MIME Certificates	S/MIME Certificates issued under this CPS are validated as to the email address only. Applicants may populate other fields of the Certificate request such as name and company, but this information is not validated in any way by Trustwave, nor shall it be contained within the final Certificate issued by Trustwave. Trustwave will confirm that the Applicant holds the private key corresponding to the public key to be included in the Certificate. Trustwave performs a limited confirmation of the Certificate Applicant's e-mail address through the following request/response mechanism: • Trustwave receives an request for an S/MIME Certificate. • Trustwave will send an email to the email address provided in the Certificate request with a unique link that the Applicant shall click on in order to retrieve their S/MIME Certificate. • The Applicant shall click on the link which will take them to a webpage. • The Applicant then confirms their information and clicks a button asking for the Certificate to be issued. • The Certificate is then issued and provided to the Subscriber in the form of a download link. • The Subscriber clicks on the download link and then saves the Certificate file and installs it according to the instructions for their operating platform.

3.2.4 Non-Verified Subscriber Information

All information contained within digital Certificates issued by Trustwave will be verified, except as it may have otherwise been stated in section 3.2.3 for S/MIME Certificates or in relation to Qualified Certificates issued pursuant to the requirements of the European Directive 99/93.

3.2.5 Validation of Authority

EV Certificates, EV Code Signing Certificates, Organizational CA Certificates	**Verification of Contract Signer / Certificate Approver** For both the Contract Signer and the Certificate Approver, Trustwave shall verify each of the following: i. the name and title of the Contract Signer and the Certificate Approver, as applicable. Trustwave shall also verify that the Contract Signer and the Certificate Approver are agents representing Applicant; ii. through a source other than the Contract Signer, that the Contract Signer is expressly authorized by Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of Applicant, including a contract that designates one or more Certificate Approvers on behalf of Applicant ("Signing Authority"); iii. through a source other than the Certificate Approver, that the Certificate Approver is expressly authorized by Applicant to do each of the following, as of the date of the Certificate Request: 1. Submit, and, if applicable, authorize a Certificate Requester to submit, the Certificate Request on behalf of Applicant; and 2. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from Applicant by the CA for issuance of the Certificate; and 3. Approve Certificate Requests submitted by a Certificate Requester. Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include: i. Name and Title. Trustwave may verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable

	assurance that a person claiming to act in such a role is in fact the named person designated to act in such role. ii. Agency. Trustwave may verify agency of the Contract Signer and the Certificate Approver by: 1. Contacting Applicant's Human Resources Department by phone or mail (at the phone number or address for Applicant's Place of Business, verified in accordance with these CA/Browser Forum EV Guidelines) and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee; or 2. Obtaining an Independent Confirmation From Applicant, or a Verified Legal Opinion, or a Verified Accountant Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either an employee or has otherwise been appointed as an agent of Applicant; or 3. Trustwave may also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the Trustwave and Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified. Acceptable methods of verification of the Signing Authority of the Contract Signer, and the authority of the Certificate Approver, as applicable, include: i. Legal Opinion. The Signing Authority of the Contract Signer, and/or the authority of the Certificate Approver, may be verified by reliance on a Verified Legal Opinion; or ii. Accountant Letter. The Signing Authority of the Contract Signer, and/or the authority of the Certificate Approver, may be verified by reliance on a Verified Accountant Letter; or iii. Corporate Resolution. The Signing Authority of the Contract Signer, and/or the authority of the Certificate Approver, may be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (1) certified by the appropriate corporate officer (e.g., secretary), and (2) Trustwave can reliably verify that the certification was validly signed by such person, and that such person

	does have the requisite authority to provide such certification; or iv. Independent Confirmation from Applicant The Signing Authority of the Contract Signer, and/or the authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation from Applicant; or v. Contract between Trustwave and Applicant. The authority of the Certificate Approver may be verified by reliance on a contract between the Trustwave and Applicant that designates the Certificate Approver with such authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified. Pre-Authorized Certificate Approver. Where Trustwave and Applicant contemplate the submission of multiple future Certificate Requests, then, after Trustwave has verified both of the following: i. the name and title of the Contract Signer and that he/she is an employee or agent of Applicant, and ii. the Signing Authority of such Contract Signer in accordance with one of the procedures set forth above, then Trustwave and Applicant may enter into a written agreement, signed by the Contract Signer on behalf of Applicant, whereby, for a specified term, Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise authority with respect to each future Certificate Application submitted on behalf of Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s). Such an agreement shall provide that Applicant shall be obligated under the Subscriber Agreement for all Certificates issued at the request of, or approved by, such Certificate Approver(s) until such authority is revoked, and shall include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when Certificate Requests are approved, (ii) periodic re-confirmation of the authority of the Certificate Approver, (iii) secure procedures by which Applicant can notify Trustwave that the authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.
OV Certificates	See 3.2.2
OV Code Signing Certificates	See 3.2.2

S/MIME Certificates	No stipulation.

3.2.6 Criteria for Interoperation

No stipulation.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

Prior to the expiration of an existing Subscriber's Certificate, it may be necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. This process is defined as Cerificate Re-key. Subscribers shall generate a new Key Pair to replace the expiring Key Pair. For purposes of this CPS, and for all Certificates issued within the TPH, Renewal Certificate Applications are subject to the same authentication steps outlined in this CPS as they apply to initial issuance of a Certificate. Expiring Certificates are not revoked by Trustwave upon issuance of the renewal Certificate. The Subscriber shall pay the fees and comply with the other terms and conditions for renewal as presented on Trustwave's Web site.

3.3.2 Identification and Authentication for Re-key after Revocation

There is no Re-key after revocation. After revocation a Subscriber shall submit a new Application.

3.4 Identification and Authentication for Revocation Request

3.4.1 Circumstances For Revocation

Certificate revocation is the process by which Trustwave prematurely ends the Validity Period of any Certificate by posting the serial number of the Certificate to a Certificate Revocation List. Trustwave will revoke a Certificate when any of the following events set forth in section 4.9.1 occur. Prior to the revocation of a Certificate, Trustwave verifies that the Certificate's Subscriber is the entity requesting such revocation.

3.4.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by Trustwave is the Subscriber, which includes its designated representatives, Certificate Approver, and the Contract Signer.

3.4.3 Procedure For Revocation Request

See section 4.9.3.

4. CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

This CPS includes operational aspects of our Certification Authority that pertain to all types of Certificates issued from the Root CA Certificates governed by this CPS.

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application

Applications can be submitted by anyone who complies with the provisions specified in the registration form, CP/CPS and relevant End-User Agreements.

EV Certificates	Applications for EV Certificates shall be requested by employees of an organization such that they meet the requirements of section 3 .2.5 Validation of Authority.
EV Code Signing Certificates	Applications for EV code signing Certificates shall be requested by an employee of an organization that meets the requirements of section 3.2.5 Validation of Authority.
OV Certificates	Applications for OV Certificates shall be submitted by either 1) the administrative or technical contact associated with WHOIS record for the domain, or 2) Trustwave shall verify the Certificate Approver is expressly authorized by the Applicant by one of the following: a.) A Verified Legal Opinion or Verified Accountant Letter which states that the Certificate requester has Certificate requesting authority; b.) Trustwave can obtain a corporate resolution from Applicant which states the Certificate requester has the Certificate requesting authority. This resolution shall be certified by appropriate company officer, and Trustwave shall be able to reliably verity the company officer has signed the resolution and that he/she has the authority to sign the resolution; c.) Trustwave can obtain confirmation from the Applicant which states the Contract Signer has the signing authority and the Certificate Approver has the requesting authority; or d.) Trustwave and Applicant may mutually enter into a contract which states that the Certificate requester has requesting authority.
OV Code Signing Certificates	Applications for OV Code Signing Certificates shall be submitted by the Certificate Approver who is expressly authorized by the Applicant by one of the following: a.) A Verified Legal Opinion or Verified Accountant Letter which states that the Certificate requester has Certificate requesting authority; b.) Trustwave can obtain a corporate resolution from Applicant which states the Certificate requester has the Certificate requesting authority. This resolution shall be certified by appropriate company officer, and Trustwave shall be able to reliably verity the company officer has signed the resolution

	and that he/she has the authority to sign the resolution; c.) Trustwave can obtain confirmation from the Applicant which states the Contract Signer has the signing authority and the Certificate Approver has the requesting authority; or d.) Trustwave and Applicant may mutually enter into a contract which states that the Certificate requester has requesting authority.
S/MIME Certificates	No stipulation.
Organizational CA Certificates	Applications for subordinate certification authority Certificates shall be requested by an employee of an organization that meets the requirements of section 3.2.5 Validation of Authority

4.1.2 Enrollment Process and Responsibilities

EV Certificates, EV Code Signing Certificates, Organizational CA Certificates	Role Requirements. The following Applicant roles are required for the issuance of an EV, EV code signing, or subordinate CA Certificate. a.) Certificate Requester – The Certificate Request shall be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits a Certificate Request on behalf of the Applicant. b.) Certificate Approver – The Certificate Request shall be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters. c.) Contract Signer – A Subscriber Agreement applicable to the requested Certificate shall be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either Applicant, employed by Applicant, or an authorized agent who has express authority to represent Applicant, and who has authority on behalf of Applicant to sign Subscriber Agreements. One person may be authorized by Applicant to fill one, two, or all three of these roles, provided that the Certificate Approver and Contract Signer are employees of Applicant. An Applicant may

	also authorize more than one person to fill each of these roles. Following completion of contract arrangements as per section 3.2.5, the applicant shall submit a PKCS #10 Certificate Signing Request ("CSR") for initial application processing.
OV Certificates, OV Code Signing Certificates, S/MIME Certificates	Applicants for OV Certificates to be issued by Trustwave shall follow the registration procedures as defined by the Trustwave. The primary steps for a Certificate registration are: 1. Valid identification documentation is provided and complete registration forms have been signed; 2. The CP's/CPS and End-User Agreement have been accepted by the Subscriber; and 3. All documents and information provided by Applicant are approved by Trustwave.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

EV Certificates, Organizational CA Certificates	Before issuing a Certificate, Trustwave shall ensure that all Subject organization information in the Certificate conforms to the requirements of, and has been verified in accordance with, the CA/Browser Forum Guidelines and matches the information confirmed and documented by Trustwave pursuant to the verification processes. The verification process shall accomplish: 1. Verification of Applicant's existence and identity, including: • Verify Applicant's legal existence and identity • Verify Applicant's physical existence • Verify Applicant's operational existence 2. Verify Applicant is a registered holder or has exclusive control of the domain name 3. Verify Applicant's authorization for requesting the Certificate including: • Verify the name, title, and authority of the contract signer, Certificate Approver, and Certificate Requester. • Verify that Contract Signer signed the Subscriber Agreement, and • Verify that a Certificate Approver has signed or otherwise approved the Certificate request Maximum Validity Period for Validated Data The age of validated data used to support issuance of a Certificate (before revalidation is required) shall not exceed the following limits: (1) Legal existence and identity – one year; (2) Assumed name – one year; (3) Address of Place of Business – one year, but thereafter

	data MAY be refreshed by checking a Qualified Independent Information Source (4) Telephone number for Place of Business – one year; (5) Bank account verification – one year; (6) Domain name – one year; (7) Identity and authority of Certificate Approver – one year, unless a contract is in place between Trustwave and Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract MAY use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated. Note on Reuse and Updating Information and Documentation (a) Use of Documentation to Support Multiple EV Certificates Trustwave may, at its own discretion, issue multiple Certificates listing the same Subject and based on a single EV Certificate Request, subject to the aging and updating requirement in (b) below. (b) Use of Pre-Existing Information or Documentation (1) Each EV Certificate issued by Trustwave must be supported by a valid current EV Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of Applicant. (2) The age of information used by Trustwave to verify such an EV Certificate Request shall not exceed the Maximum Validity Period, as defined above, for such, based on the earlier of the date the information was obtained (e.g., the date of a confirmation phone call) or the date the information was last updated by the source (e.g., if an online database was accessed by Trustwave on July 1, but contained data last updated by the vendor on February 1, then the date of information would be considered to be February 1). (3) In the case of outdated information, Trustwave shall repeat the verification processes required in this CPS.
EV Code Signing Certificates,	Before issuing an EV Code Signing Certificate, Trustwave shall ensure that all Subject organization information in the Certificate conforms to the requirements of, and has been verified in the same manner as EV Certificates, except that domain name verification is not performed.
OV Certificates	When a Subscriber does not have a pre-existing Certificate, prior to issuing the Subscriber its new Certificate, Trustwave shall validate (a) the Applicant's organizational data and (b) their domain name information to make sure that the information contained in their Certificate request properly matches information made available in publicly available databases, or matches information provided by the Subscriber via facsimile, email, or

	over the telephone. Trustwave may use any combination of validation procedures to validate this information, and organizational information may be validated in a different fashion and at a different time then the domain name information, however, both the organizational information and the domain name information shall be validated prior to a Certificate being issued by Trustwave. Once both the organizational information and the domain name information are validated, the Subscriber's Certificate will be issued.
OV Code Signing Certificates	When a Subscriber does not have a pre-existing Certificate, prior to issuing the Subscriber its new Certificate, Trustwave shall validate the Applicant's organizational to make sure that the information contained in their Certificate request properly matches information made available in publicly available databases, or matches information provided by the Subscriber via facsimile, email, or over the telephone. Trustwave may use any combination of validation procedures to validate this information. However, all organizational information shall be validated prior to a Certificate being issued by Trustwave. Once the organizational information is validated, the Subscriber's Certificate will be issued.
S/MIME Certificates	S/MIME Certificates issued under this CPS are validated as to the email address only. Applicants may populate other fields of the Certificate request such as name and company, but this information is not validated in any way by Trustwave. Trustwave will confirm that the Applicant holds the private key corresponding to the public key to be included in the Certificate. Trustwave also performs a limited confirmation of the Certificate Applicant's e-mail address following the request/response mechanism in 3.2.3.

4.2.2 Approval or Rejection of Certificate Applications

The approval or rejection of a Certificate request is made following satisfactory completion of all requirements in 4.2.1. An approval requires that the Applicant be in good payment standing.

4.2.3 Time to Process Certificate Applications

The following are the average timelines for completion of a Certificate Request and issuance of a Certificate:

- EV Certificates, EV Code Signing Certificates, Organizational CA Certificates – 10 business days
- OV Certificates, OV Code Signing Certificates – 2 business days
- S/MIME Certificates – 1 business day

4.3 Certificate Issuance

4.3.1 CA Actions During Certificate Issuance

Following successful completion of all relevant sections within 3.1 and 4.2, Trustwave, as determined in its sole discretion, will approve the Certificate application and issue the Subscriber's Certificate.

4.3.1.1 CA Actions for Non-Latin Organization Name Encoding

Where an EV Applicant's organization name is not registered with a QGIS in Latin characters and the applicant's foreign character organization name and registration have been verified with a QGIS in accordance with this CPS, Trustwave may include a Latin character organization name in an EV certificate. In such a case, Trustwave shall comply with the following process.

In order to include a transliteration/Romanization of the registered name, the Romanization shall be verified by Trustwave using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation. If Trustwave cannot rely on a transliteration/Romanization of the registered name using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation, then Trustwave shall rely on one of the options below, in order of preference:

(a) A system recognized by the International Standards Organization (ISO),
(b) A system recognized by the United Nations, or
(c) A Lawyer's Opinion confirming the Romanization of the registered name.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

Trustwave shall notify the Applicant that the Certificate has been issued via either e-mail, telephone, or face-to-face contact. Once the Applicant has been notified, the Subscriber will either download the Certificate over HTTPS, or receive the Certificate via e-mail.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The Subscriber expressly indicates acceptance of a Certificate by using such Certificate or downloading and installing the Certificate.

4.4.2 Publication of the Certificate by the CA

No stipulation. Due to privacy concerns, Trustwave does not publish End-Entity Certificates in any form of a global directory.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers, for all forms of Trustwave issued digital Certificates, shall

- possess at least a rudimentary knowledge of public key cryptography and digital Certificates;

- have completed all necessary enrollment forms and have executed payment for all accounts due;
- read and agree to this CPS, any and all relevant CP's, and any and all Subscriber Agreements;
- protect their private key from unauthorized access and Compromise;
- not share their private key and or passwords protecting their private key;
- notify Trustwave of any change to the information contained within the Certificate;
- comply with all laws and regulations applicable to the export, import, and use of Certificates issued by Trustwave.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall:

- possess at least a rudimentary knowledge of public key cryptography and digital Certificates and their associated risks;
- read and agree to this CPS, any and all relevant CP's, and any and all Relying Party Agreements;
- verify, prior to using and relying on a Certificate, its validity by using CRL's (or OCSP) with correct certification path validation procedures and all critical extensions;
- comply with all laws and regulations applicable to the export, import, use and reliance on a Certificate issued by Trustwave

4.6 Certificate Renewal

Certificate renewal involves a process whereby the Subscriber retains the key pair used within a previously issued Certificate, but submits updated or current identity and/or validity information. Neither Trustwave root CAs, nor any member CA of the TPH, shall support Certificate renewal. Trustwave shall support only certificate re-key as defined in 4.7

4.6.1 Circumstance for Certificate Renewal

No stipulation.

4.6.2 Who May Request Renewal

No stipulation.

4.6.3 Processing Certificate Renewal Requests

No stipulation.

4.6.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

No stipulation.

4.6.6 Publication of the Renewal Certificate by the CA

No stipulation.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7 Certificate Re-key

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new Certificate to maintain continuity of Certificate usage. This process is defined as Certificate Re-key. Subscribers shall always generate a new key pair to replace the expiring key pair. For purposes of this CPS, Re-key Certificate Applications are subject to the same authentication steps outlined in this CPS as apply to initial issuance of a Certificate. Expiring Certificates are not revoked by Trustwave upon issuance of the new Certificate. The Subscriber shall pay the fees and comply with the other terms and conditions for renewal as presented by Trustwave, including those on Trustwave's website.

4.7.1 Circumstance for Certificate Re-key

No stipulation.

4.7.2 Who May Request Certification (Signing) of a New Public Key

No stipulation.

4.7.3 Processing Certificate Re-keying Requests

No stipulation.

4.7.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

No stipulation.

4.7.6 Publication of the Re-keyed Certificate by the CA

No stipulation.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8 Certificate Modification

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. Trustwave shall deem such request as an initial registration request. The requester is therefore required to start a new Certificate request.

4.8.1 Circumstance for Certificate Modification

No stipulation.

4.8.2 Who May Request Certificate Modification

No stipulation.

4.8.3 Processing Certificate Modification Requests

No stipulation.

4.8.4 Notification of New Certificate Issuance to Subscriber

No stipulation.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

No stipulation.

4.8.6 Publication of the Modified Certificate by the CA

No stipulation.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

Certificate revocation is the process by which Trustwave prematurely terminates the Validity Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List. Trustwave will revoke the Certificate when any of the following events occurs:

(1) The Subscriber requests revocation of its Certificate;
(2) The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
(3) Trustwave obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been Compromised, or that the Certificate has otherwise been misused;
(4) Trustwave receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
(5) Trustwave receives notice or otherwise becomes aware that a court or arbitrator has revoked a Subscriber's right to use the domain name listed in the Certificate, or that the Subscriber has failed to renew the domain name;
(6) Trustwave receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
(7) A determination, in Trustwave's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of this CPS or the applicable CP;
(8) Trustwave determines that any of the information appearing in the Certificate is not accurate;
(9) Trustwave ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
(10) Trustwave's Private Key for that Certificate has been Compromised;
(11) Such additional revocation events as Trustwave publishes; or
(12) Trustwave 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 Trustwave's jurisdiction of operation.
(13) The Subscriber intentionally includes Suspect Code in its signed software.

4.9.2 Who Can Request Revocation

The only persons permitted to request revocation of a Certificate issued by Trustwave is the Subscriber (including designated representatives; Certificate Approver, Contract Signer).

4.9.3 Procedure for Revocation Request

To request revocation, a Subscriber shall contact Trustwave, either by e-mail message, a national/regional postal service, facsimile, or overnight courier, and specifically request "revocation" (using that term) of a particular Certificate identified by the Subscriber. Upon receipt of a revocation request, Trustwave will seek confirmation of the request by e-mail message to the person requesting revocation (as defined in 4.9.2 above). The message will state that, upon confirmation of the revocation request, Trustwave shall revoke the Certificate and that posting the revocation to the appropriate CRL shall constitute notice to the Subscriber that the Certificate has been revoked. Trustwave shall require a confirming e-mail message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to Trustwave). Upon receipt of the confirming e-mail message, Trustwave shall revoke the Certificate and the revocation shall be posted to the appropriate CRL. Notification shall be sent to the subject of the Certificate and the subject's designated contacts. There is no grace period available to the Subscriber prior to revocation, and Trustwave shall respond to the revocation request within the next business day and post the revocation to the next published CRL. In the event of Compromise of Trustwave's Private Key used to sign a Certificate, Trustwave shall send an e-mail message as soon as practicable to all Subscribers with Certificates issued off the Private Key stating that the Certificates shall be revoked by the next business day and that posting the revocation to the appropriate CRL shall constitute notice to the Subscriber that the Certificate has been revoked.

4.9.4 Revocation Request Grace Period

See 4.9.3

4.9.5 Time within Which CA Must Process the Revocation Request

See 4.9.3

4.9.6 Revocation Checking Requirement for Relying Parties

No stipulation.

4.9.7 CRL Issuance Frequency

CRL's shall be issued by all certification authorities within the TPH on a daily basis.

4.9.8 Maximum Latency for CRLs

As per 4.9.7, all CRL's issued by certification authorities within the TPH shall be issued on a daily basis and without delay. The maximum latency for any CRL shall be one day.

4.9.9 On-line Revocation/Status Checking Availability

No stipulation.

4.9.10 On-line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Regarding Key Compromise

No stipulation.

4.9.13 Circumstances for Suspension

No certification authority within the TPH shall suspend Certificates.

4.9.14 Who Can Request Suspension

No stipulation. See 4.9.13

4.9.15 Procedure for Suspension Request

No stipulation. See 4.9.13

4.9.16 Limits on Suspension Period

No stipulation. See 4.9.13

4.10 Certificate Status Services

No stipulation. Currently, Trustwave does not provide OCSP services.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Trustwave shall attempt to notify all Subscribers of the expiration date of their Certificate. Notifications will generally be by e-mail message to the administrative / Certificate Requester contacts listed during enrollment submitted by the Certificate Requester, and will likely occur periodically during the 90 day period prior to the expiration date and the 14 day period following the expiration date. If the Subscriber's enrollment form was submitted by another party on the Subscriber's behalf, Trustwave may not send expiration notices to that party. Trustwave is not responsible for ensuring that the customer is notifed prior to the expiration of their Certificate.

4.12 Key Escrow and Recovery

Trustwave does not provide nor perform any form of key escrow or recovery services. No certification authority within the TPH shall escrow their private keys. Certification authorities within the ORGCA hierarchy may escrow private keys issued to their Subscribers if the following guidelines are met:

- A documented escrow design including all protection facilities shall be provided to Trustwave; and
- All escrowed keys SHALL NOT have the digital signature or non-repudiation bits set within the private key's key usage extension associated with the digital Certificate.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical Controls

5.1.1 Site Location and Construction

Trustwave CA operations are conducted within a physically secure environment that deters, prevents, and detects unauthorized use of, access to, or disclosure of sensitive information and systems whether covert or overt.

Trustwave maintains "cold" disaster recovery systems at a geographically separate facility for its CA operations. The systems do not contain key material and are kept off-line and are stored in a physically secure manner. The disaster recovery procedures are detailed further in Section 5.7.

5.1.2 Physical Access

Physical Access is restricted to the secure server room. The room can only be accessed through dual-access controls which require that two persons be present and utilize two distinct methods of access consisting of a combination of PIN numbers, proximity cards, and Keys. The system has been designed so that entry by a single individual is not possible.

5.1.3 Power and Air Conditioning

Trustwave's facility is equipped with primary and backup:

- power systems to ensure the operation of its servers and its network connections; and
- HVAC systems to control temperature and relative humidity.

5.1.4 Water Exposures

Trustwave has taken reasonable precautions to minimize the impact of water exposure to its systems.

5.1.5 Fire Prevention and Protection

Trustwave has taken reasonable precautions to prevent fires and has fire suppression equipment available on-site.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within Trustwave facilities or in a secure off-site storage facility with appropriate physical and logical access controls designed to limit access to authorized personnel and protect such media from accidental damage (e.g., water, fire, and electromagnetic).

5.1.7 Waste Disposal

Sensitive documents and materials are shredded before disposal. Media used to collect or transmit sensitive information are rendered unreadable before disposal. Cryptographic devices are physically destroyed or zeroed in accordance with the

manufacturer's guidance prior to disposal. Other waste is disposed of in accordance with Trustwave's normal waste disposal requirements.

5.1.8 Off-site Backup

Trustwave performs routine backups of critical system data, audit log data, and other sensitive information. This information is stored in a physically secure location geographically separate from the main CA facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

Trusted Persons include all employees, contractors, and consultants that have access to or control authentication or cryptographic operations that may materially affect:

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;
- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository; and
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- customer service personnel;
- cryptographic business operations personnel;
- security personnel;
- system administration personnel;
- designated engineering personnel; and
- executives that are designated to manage infrastructural trustworthiness.

Trustwave considers the categories of personnel identified in this section as Trusted Persons having a Trusted Position. Persons seeking to become Trusted Persons by obtaining a Trusted Position shall successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

Trustwave has established, maintains, and enforces rigorous control procedures to ensure the segregation of duties based on job responsibility and to ensure that multiple Trusted Persons are required to perform sensitive tasks.

Policy and control procedures are in place to ensure segregation of duties based on job responsibilities. The most sensitive tasks, such as access to and management of CA cryptographic hardware (Hardware Security Module or HSM) and associated key material require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two Trusted Persons are required to have either physical or logical access to the device. Access to CA cryptographic hardware is strictly enforced by multiple Trusted Persons throughout its lifecycle, from incoming receipt and inspection to final logical and/or physical destruction. Once a module is activated with

operational keys, further access controls are invoked to maintain split control over both physical and logical access to the device.

5.2.3 Identification and Authentication for Each Role

For all personnel seeking to become Trusted Persons, verification of identity is performed through the personal (physical) presence of such personnel before Trusted Persons performing Trustwave HR or security functions and a check of well-recognized forms of identification (e.g., passports and driver's licenses). Identity is further confirmed through the background checking procedures in Section 5.3.1.

Trustwave ensures that personnel have achieved Trusted Status and departmental approval has been given before such personnel are:

- issued access devices and granted access to the required facilities;
- issued electronic credentials to access and perform specific functions on Trustwave CA, RA, or other IT systems.

5.2.4 Roles Requiring Separation of Duties

Roles requiring Separation of duties include (but are not limited to):

- the generation, issuing, backups, or destruction of a Root CA key pair;
- the loading of Root CA Keys on an HSM;
- the storage of or access to Root CA Key Material; and
- access to all CA private keys for the purposes of Certificate issuance.

5.3 Personnel Controls

5.3.1 Qualifications, Experience, and Clearance Requirements

Consistent with this CPS, Trustwave maintains personnel and management practices that provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. Additionally, Trustwave shall maintain the following practices.

1. Trustwave shall provide all employees and contractors interacting with the TPH with annual skills training that covers basic public key infrastructure knowledge, authentication and verification policies and procedures, and overview of common threats to the validation process, and this certification practice statement itself.
2. Trustwave shall maintain all records associated with training of the employees and contractors within the TPH for seven years.
3. Individuals responsible for the progression of initially gathering, then validating, subsequently approving, and finally auditing information, associated with any Certificate issuance process, shall qualify for each skill level prior to advancing to the next. This qualification will consist of an internally administered examination.

5.3.2 Background Check Procedures

Trustwave requires its employee to undergo a successful completion of background investigation which includes the following:

- Social Security Number Verification;
- Criminal Records Search;
- Credit History Review;
- Education Verification;
- Employment History Verification; and
- Foreign Records Search.

5.3.3 Training Requirements

Trustwave provides all personnel performing validation duties ("Validation Specialists") with skills training that covers basic Public Key Infrastructure (PKI) knowledge, authentication and verification policies and procedures, common threats to the validation process, including phishing and other social engineering tactics, this CPS, and all CA/Browser Forum Guidelines.

5.3.4 Retraining Frequency and Requirements

All Trustwave employees and contractors interacting with the TPH shall undergo an annual retraining exercise.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Failure of any Trustwave employee or agent to comply with the provisions of this CPS, whether through negligence or malicious intent, will subject such individual to appropriate administrative and disciplinary actions, which may include termination as an employee or agent and possible civil and criminal sanctions.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles interacting with any component of the TPH are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8 Documentation Supplied to Personnel

Employees and contractors in trusted roles are provided with the documentation necessary to perform the role to which they are assigned, including a copy of this CPS and all technical and operational documentation needed to maintain the integrity of the TPH CA operations.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

In addition to standard best practice system auditing procedures, Trustwave shall maintain records that include documenting:

- Compliance with this CPS and other obligations under Trustwave agreements with subscribers
- All actions, information, and events material to the enrollment, creation, issuance, use, expiration, and revocation of all Certificates issued by Trustwave

Specifically, Trustwave shall record the following events:

- CA key lifecycle management events, including:
    - Key generation, backup, storage, recovery, archival, and destruction; and
    - Cryptographic device lifecycle management events.
- CA and Subscriber Certificate lifecycle management events, including:
    - EV Certificate Requests, renewal requests, re-key requests, and revocation;
    - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    - Acceptance and rejection of Certificate Requests;
    - Issuance of Certificates; and
    - Generation of Certificate Revocation Lists (CRLs) and OCSP entries.
- Security events, including:
    - Successful and unsuccessful PKI system access attempts;
    - PKI and security system actions performed;
    - Security profile changes;
    - System crashes, hardware failures, and other anomalies;
    - Firewall and router activities; and
    - Entries to and exits from the CA facility.

5.4.2 Frequency of Processing Log

Trustwave shall review the content of all logs at least a weekly basis. Follow-ups to all exceptions are required.

5.4.3 Retention Period for Audit Log

Trustwave shall maintain the written reviews of all audit log analysis for at least seven years.

5.4.4 Protection of Audit Log

Trustwave shall perform best effort mechanisms to protect all audit logs, including but not limited to:

- Network segregation
- Network intrusion detection systems,
- Network firewalls, and
- Antivirus systems (where applicable).

In addition, Trustwave shall deploy system-level access control such that only individuals with a “need to know” shall be able to view audit logs.

5.4.5 Audit Log Backup Procedures

Trustwave, and all certification authority members of the TPH, shall perform daily backup operations for all systems, including systems responsible for log collection.

5.4.6 Audit Collection System (Internal vs. External)

No stipulation.

5.4.7 Notification to Event-Causing Subject

No stipulation.

5.4.8 Vulnerability Assessments

Trustwave performs monthly vulnerability scanning across the Trustwave managed certification authority infrastructure.

5.5 Records Archival

5.5.1 Types of Records Archived

In addition to the audit logs specified above, Trustwave shall maintain records that include documenting the following.

- All Certificate issuance records are retained as records in electronic and/or in paper-based archives for the period detailed below in Section 5.5.2. Copies of Certificates are held, regardless of their status as expired or revoked;
- All appropriate documentation submitted by Applicants in support of a Certificate application;
- All records associated with Certificate issuance as part of its Certificate;
    - Approval checklist process
    - the Subscriber's PKCS#10 CSR;
    - documentation of organizational existence for organizational applicants as listed in Section 3.2.2;
    - documentation of individual identity for individual Applicants;
    - verification of organizational existence and status received from third party databases and government entities (including screen shots of web sites reporting such information);
    - screen shot of WHOIS record for domain name to be listed in the Certificate;
    - mailing address validation (if different than those identified through the resources listed above);
    - letter of authorization for web sites managed by third party agents of Applicants (if applicable);
    - submission of the Certificate application, including acceptance of the Subscriber Agreement;
    - name, e-mail, and IP address of person acknowledging authority of the Contract Signer and Approver;
    - other relevant contact information for the Applicant/Subscriber; and
    - copies of Digital Certificates issued.

5.5.2 Certificate Revocation

Requests for Certificate revocation are recorded and archived, including the name of the person requesting revocation, the reason for the request and the Trustwave personnel involved in authorizing revocation. This information and all resulting CRL's are retained as records in electronic archives for the period detailed in Section 5.5.3 below.

5.5.3 Retention Period for Archive

Trustwave retains the records of all certification authority activities and the associated documentation for a term of no less than 7 years.

5.5.4 Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution or destruction.

5.5.5 Archive Backup Procedures

No stipulation.

5.5.6 Requirements for Time-stamping of Records

All system time settings for all components within the Trustwave managed TPH utilize the Network Time Protocol (NTP) with synchronization on at least a daily basis. All archives and log entries shall utilize the local network time provider which has been synchronized via NTP.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

5.6 Key Changeover

Trustwave shall cease using any certification authority key one year prior to its expiration. After such time, the sole use for this key shall be to sign CRL's. A new CA signing key pair shall be commissioned, and all subsequently issued Certificates and CRL's are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If any CA within the TPH has its private key (or suspected to be) compromised, Trustwave shall:

- Inform all subscribers and relying parties of which the CA is aware.
- Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

5.7.2 Entity Private Key Compromise Procedures

If any CA within the TPH has its private key (or suspected to be) compromised, Trustwave shall:

- notify all subordinate CA's;
- make a reasonable effort to notify subscribers;
- terminate issuing and distribution of Certificates and CRL's;
- request revocation of the compromised Certificate; and
- generate a new CA key pair and Certificate and publish the Certificate in the Repository.

5.7.3 Business Continuity Capabilities After a Disaster

Trustwave maintains several documented disaster recovery and business continuity plans for use in the case of a declared disaster. All certification

authorities managed by Trustwave within the TPH shall adhere to and follow these plans in the case of a declared disaster associated with any certification authority. These plans are as follows:

- Trustwave IT Disaster Recovery Plan (current: version 3.0, October 2007)
- Trustwave Business Continuity Plan (current: version 1.0, October 2007)
- MING System Disaster Recovery Plan (current: version 1.0, October 2007).

5.8 CA or RA Termination

In the event that Trustwave or its CA's cease operating, Trustwave shall make a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance. If practicable, Trustwave will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties;
- Informing such parties of the status of the CA;
- Handling the cost of such notice;
- The preservation of the CA's archives and records for the time periods required in this CPS;
- The continuation of Subscriber and customer support services;
- The continuation of revocation services, such as the issuance of CRL's;
- The revocation of unexpired, unrevoked Certificates of Subscribers and subordinate CAs, if necessary;
- The payment of compensation (if necessary) to Subscribers whose unexpired, unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA;
- Disposition of the CA's Private Key and the hardware tokens containing such Private Key;
- Provisions needed for the transition of the CA's services to a successor CA; and
- The identity of the custodian of Trustwave's CA and RA archival records.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

CA Key Pair generation is performed by multiple trained and trusted individuals using secure systems and processes that provide for the security and required cryptographic strength for the keys that are generated. All CA Key Pairs are generated in pre-planned key generation ceremonies in accordance with the requirements of Trustwave security and audit requirements guidelines and the CA/Browser Forum Guidelines. The activities performed in each key generation ceremony are recorded, dated, and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by Trustwave management.

Trustwave CA Key Pairs are maintained in a trusted and highly secured environment with backup and key recovery procedures. In the event of the Compromise of one or more of the Trustwave Key(s), Trustwave shall promptly notify all Subscribers via e-mail and notify Relying Parties and others via the CRL and additional notice posted at http://www.trustwave.com/CA. Trustwave shall also revoke all Certificates issued with such Trustwave CA Key(s).

When Trustwave CA Key Pairs reach the end of their Validity Period, such CA Key Pairs will be archived for a period of at least 7 years. Archived CA Key Pairs will be securely stored using off-line media. Procedural controls will prevent archived CA Key Pairs from being returned to production use. Upon the end of the archive period, archived CA Private Keys will be securely destroyed. Trustwave CA Key Pairs are retired from service at the end of their respective maximum lifetimes as defined above. This helps to ensure there is no key changeover. Certificates may be renewed as long as the cumulative certified lifetime of the Certificate Key Pair does not exceed the maximum CA Key Pair lifetime. New CA Key Pairs will be generated as necessary, for example to replace CA Key Pairs that are being retired, to supplement existing, active Key Pairs and to support new services in accordance with this CPS.

6.1.1 Key Pair Generation

6.1.1.1 Trustwave Certification Authority Key Pair Generation

All Trustwave managed certification authority key pairs shall be:

1. Generated in hardware security modules as defined in section 6.2;
2. RSA key pairs of at least 2048 bit size;
3. Performed in accordance with a documented key generation ceremony that is either audited by the current Web Trust auditor or videotaped. Following completion of the ceremony, all Trustwave employees present shall attest in signatory form to the adherence of the procedure. These records shall be kept for seven years; and
4. Performed by multiple trusted and qualified Trustwave employees.

6.1.1.2 Subscriber key pair generation

Trustwave does not perform Subscriber key pair generation. All and the entity keys shall be performed within the Subscribers infrastructure. Trustwave does not mandate storage of private keys within hardware security modules for Subscribers.

All private keys managed by Subscribers for subordinate certification authorities underneath ORGCA shall be managed and protected with a minimum of Federal Information Processing Standard (FIPS) 140-2 Level 2 hardware security module.

6.1.2 Private Key Delivery to Subscriber

Trustwave does not perform private key generation or delivery to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

If Trustwave finds all of the information and material supplied by the Applicant to be sufficiently verified, a Certificate will be issued to the Applicant by Trustwave. Upon issuance of the Applicant's Certificate, Trustwave will attach such Certificate to an e-mail and send such e-mail to the appropriate contacts. The e-mail will typically be sent only to the verified Certificate requester. In certain circumstances the e-mail may include a Trustwave customer service representative telephone number and e-mail address for any technical or customer service problems. Trustwave, in its sole discretion, may provide such technical or customer support to the Applicants/Subscribers.

Trustwave may also deliver the Subscriber's signed Certificate via an online account download or through an Application Programming Interface (API).

6.1.4 CA Public Key Delivery to Relying Parties

Relying Parties can find Trustwave root certification authority Certificates within commonly used operating systems and browsers. Relying Parties may also obtain Trustwave certification authority root Certificates from https://ssl.trustwave.com/CA.

6.1.5 Key Sizes

All certification authorities within TPH shall use at least 2048 bit RSA keys. Trustwave accepts CSR's of Applicants that use at least 1024 bit RSA keys.

6.1.6 Public Key Parameters Generation and Quality Checking

The public exponent of all participants within the TPH shall use a public exponent of 3, 17, or 65,537 for the generation of their RSA key pair. All hardware security modules are used for storage of Trustwave managed certification authority keys shall be FIPS 186-2 compliant and shall provide hardware-based random number generation.

6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field)

All Certificates within the TPH shall contain the X.509 v3 key usage field so that the usage of the private key can be delimited and determined by X.509 compliant software. In addition, the Subscriber and End-Entity Certificates may have extended key usage extensions set.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic Module Standards and Controls

All private keys within the Trustwave managed component of the TPH shall be protected via Federal Information Processing Standard (FIPS) 140-2 Level 3 hardware security modules.

All private keys managed by Subscribers for subordinate certification authorities underneath ORGCA shall be managed and protected with a minimum of Federal Information Processing Standard (FIPS) 140-2 Level 2 hardware security modules.

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

Access, both electronic and physical, to all private keys associated with the Trustwave managed TPH require a minimum of two Trustwave employees to come together in order to derive the private key.

6.2.3 Private Key Escrow

Trustwave does not, nor has the facilities to, escrow private keys.

6.2.4 Private Key Backup

All private key backups for the certification authorities of the TPH shall be stored in password or PIN protected hardware (smart cards) in a form such that it requires at least two trusted and qualified Trustwave employees to come together in order to regenerate the private key.

All private key backups of the following three global root certification authorities – SGCA, XGCA, and STCA shall be stored in hardware such that it requires three people to come together in order to regenerate the private key.

6.2.5 Private Key Archival

Trustwave does not archive private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

All Trustwave managed certification authority key pairs that are transferred into or from a cryptographic module shall be:

1. Performed in accordance with a documented key movement ceremony that is either audited by the current WebTrust auditor or videotaped. Following completion of the ceremony, all Trustwave employees present shall attest in signatory form to the adherence of the procedure. These records shall be kept for seven years; and
2. Performed by multiple (at least three) trusted and qualified Trustwave employees.

6.2.7 Private Key Storage on Cryptographic Module

See 6.2.1

6.2.8 Method of Activating Private Key

All End-Entities and Subscribers are solely responsible for protection of their private keys. All End-Entities and subscribers are responsible for protection of their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use. Trustwave maintains no role in the generation, protection, or maintenance of Subscriber private keys.

All Trustwave managed TPH components require multiple individuals (at least two) to come together in order to activate a certification authority's private key. This is enforced by both operating system access control and hardware security module routines.

6.2.9 Method of Decertification, Deactivating Private Key

The private keys stored on) hardware security modules are deactivated via the hosting operating systems and shut down and by lockout receivers associated with the HSM. Subscribers should also deactivate their private keys via logout and removal procedures when they are not in use.

6.2.10 Method of Destroying Private Key

At the conclusion of any certification authority's private key lifetime, the private key associated with the TPH component shall be destroyed following vendor recommended guidelines for the hardware security module.via incineration of the HSM.

6.2.11 Cryptographic Module Rating

See 6.2.1

6.3 Other Aspects of Key Pair Management

6.3.1 Public Key Archival

Trustwave retains copies of all Public Keys for archival in accordance with Section 5.5.

6.3.2 Certificate Validity Periods and Key Pair Usage Periods

All Certificates and corresponding keys shall have maximum Validity Periods (not exceeding):

- Root CA --31 years (XGCA, STCA, SGCA)
    - Newly generated root CA's – 30 years
- Trustwave managed subordinate CA – 25 years
- EV SSL Certificates—27 months
- Non-EV SSL Certificates – 39 months
- EV and Non-EV Code Signing Certificates – 39 months

6.4 Activation Data

Trustwave deploys multiple levels of electronic and physical security controls in order to protect access to CA's private keys. Physical access to computer rooms containing CA private keys shall require at least two individuals to come together in order to deactivate the physical security controls protecting the room.

In addition, Trustwave deploys a "m out of n" secret sharing routine for electronic access to CA private keys, where "m" is greater than two and "n" is six. In other words, three of the six individuals possessing a component of the activation data must come together in order to gain access to a private key as stored in an HSM. Each of these six individuals shall have their own token necessary for insertion into the HSM in order to perform activities associated with the root certification authorities' private keys.

6.4.1 Activation Data Generation and Installation

Activation data associated with each of the tokens possessed by the six individuals capable of accessing root certification authority private keys was generated during initial installation and configuration of the hardware security modules.

6.4.2 Activation Data Protection

All activation data shall be stored on FIPS 140-2 level 3 smart cards associated with the HSM's.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

No stipulation.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Trustwave maintains within its corporate information security policy and program, significant management controls governing systems development. These controls are applied for all certification authority development activities.

6.6.2 Security Management Controls

Trustwave maintains both technical and procedural mechanisms to monitor change to all components within the TPH.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

The systems containing Trustwave's TPH all reside in highly segmented networks constrained from both the Internet and the Trustwave corporate network via multiple levels of firewalls. Interaction with outside entities shall only be performed with servers located on a demilitarized zone (DMZ). Additionally, all networks associated with certification authority operations at Trustwave shall be monitored by a network intrusion detection system. All systems associated with certification authority activities shall be hardened with services restricted to only those necessary for certification authority operations. Any change associated with the TPH shall be documented and approved via a change management system.

6.8 Time-Stamping

No Stipulation. Reserved for future use.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate Profile

(Note: Textual printouts of each Trustwave root Certificate are included in Appendix A)

7.1.1 Version Number(s)

All Certificates within the TPH shall be X.509 version 3 Certificates.

7.1.2 Certificate Extensions

7.1.2.1 TPH Certification Authority Extensions

Basic constraints

All certification authority Certificates shall include the basic constraints extension with a subject type equal to "CA" and its criticality set to "critical".

Subordinate CAs underneath ORGCA that are not managed by Trustwave shall have the path length constraint set to "0".

All basic constraints extensions within certification authority Certificates shall be marked as critical.

Key Usage

All certification authority Certificates within the TPH shall contain a key usage extension set for "Certificate signing" and "CRL signing". Additionally, this extension may contain the "off-line CRL signing" bit. This extension shall be marked as non-critical.

CRL Distribution Point

All certification authority Certificates within the TPH shall contain the location of the CRL retrieval location in the form of the "CRL distribution point" extension. Typically this extension will be in the form of an HTTP URL. This extension will be marked as "non-critical".

7.1.2.2 EV Web Server SSL Certificate extensions

All EV Certificates issued by Trustwave to a Subscriber shall include:

- Trustwave's EV OID in the certificate policies extension. Trustwave's EV OID is 2.16.840.1.114404.1.1.2.4.1.
- The basic Constraints extension, marked as Critical, with Subject Type=End Entity and Path Length Constraint=None
- The key usage, marked as non-critical, set to include Signing and Key Encipherment.
- The extended Key Usage, marked as non-critical, set equal to TLS Web Server Authentication (1.3.6.1.5.5.7.3.1). No other values within the enhanced Key Usage extension shall be set.
- The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/XXXX.crl or http://crl.trustwave.com/XXXX.crl

where XXXX represents either STCA, XGCA, or GSCA depending on the issuing root CA.

7.1.2.3 OV Web Server SSL Certificate extensions

All OV Certificates issued by Trustwave to a Subscriber shall include:

- Trustwave's OV OID in the certificate policies extension. Trustwave's OV OID is 2.16.840.1.114404.2.1.2.
- The basicConstraints extension, marked as Critical, with Subject Type=End Entity and Path Length Constraint=None
- The enhanced Key Usage, marked as non-critical, set equal to TLS Web Server Authentication (1.3.6.1.5.5.7.3.1). No other values within the enhanced Key Usage extension shall be set.
- The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/XXXX.crl or http://crl.trustwave.com/XXXX.crl where XXXX represents either STCA, XGCA, or GSCA depending on the issuing root CA.

7.1.2.4 EV Code Signing Certificate Extensions

All Code Signing Certificates issued by Trustwave to a Subscriber shall include:

- Trustwave's EV Code Signing OID in the certificate policies extension. Trustwave's EV Code Signing OID is 1.3.6.1.4.1.30360.3.3.3.4.4.3.3.
- The basicConstraints extension, marked as Critical, with Subject Type=End Entity and Path Length Constraint=None
- The enhanced Key Usage, marked as non-critical, set equal to Code Signing (1.3.6.1.5.5.7.3.3). No other values within the enhanced Key Usage extension shall be set.
- The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/CSCA.crl or http://crl.trustwave.com/CSCA.crl.

7.1.2.5 OV Code Signing Certificate Extensions

All Code Signing Certificates issued by Trustwave to a Subscriber shall include:

- Trustwave's OV Code Signing OID in the certificate policies extension. Trustwave's OV Code Signing OID is 1.3.6.1.4.1.30360.3.3.3.4.4.3.4.
- The basicConstraints extension, marked as Critical, with Subject Type=End Entity and Path Length Constraint=None
- The enhanced Key Usage, marked as non-critical, set equal to Code Signing (1.3.6.1.5.5.7.3.3). No other values within the enhanced Key Usage extension shall be set.
- The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/CSCA.crl or http://crl.trustwave.com/CSCA.crl.

7.1.2.6 S/MIME Certificate Extensions

All S/MIME Certificates issued by Trustwave to a Subscriber shall include:

- Trustwave's S/MIME OID in the certificate policies extension. Trustwave's S/MIME OID is 2.16.840.1.114404.2.2.1.

- The basicConstraints extension, marked as Critical, with Subject Type=End Entity and Path Length Constraint=None
- The enhanced Key Usage, marked as non-critical, set equal to Secure Email (1.3.6.1.5.5.7.3.4). No other values within the enhanced Key Usage extension shall be set.
- The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/XXXX.crl or http://crl.trustwave.com/XXXX.crl where XXXX represents either STCA, XGCA, or GSCA depending on the issuing root CA.

7.1.2.7 Trustwave Time Stamp Authority ("TSA")

No stipulation. Reserved for future use.

7.1.3 Algorithm Object Identifiers

All Certificates issued by certification authorities within the TPH shall use RSA signatures with SHA-1 hashes for their signatures in compliance with the Internet Engineering Task Force's Request for Comment ("RFC") 3279.

7.1.4 Name Forms

Trustwave Certificates are populated using X.500 naming conventions.

7.1.5 Name Constraints

No stipulation. Reserved for future use.

7.1.6 Certificate Policy Object Identifier

Each Certificate issued by Trustwave shall contain an OID reflecting Certificate type and its associated governance as defined in section 1.1.

7.1.7 Usage of Policy Constraints Extension

No stipulation. Reserved for future use.

7.1.8 Policy Qualifiers Syntax and Semantics

No stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

For each of the nine certification authorities managed by Trustwave within the TPH, CRL's conforming to RFC 5280 shall be issued on a daily basis containing:

- Version (set to "1" in order to indicate version 2);
- Issuer Signature Algorithm (SHA-1 with RSA Encryption {1 2 840 113549 1 1 5});
- Issuer Distinguished Name (the issuing certification authority);
- This Update in ISO 8601 format with UTC designation.
- Next Update in ISO 8601 format with UTC designation;
- The list of revoked Certificates including reason code;

- Serial Number;
- Revocation Date;
- RSA Signature of the CRL.

7.2.1 Version Number(s)

Trustwave issues version 2 CRL's for all certification authorities within the TPH.

7.2.2 CRL and CRL Entry Extensions

Each Certificate revocation list issued by Trustwave may contain:

- CRL Number (unique);
- Authority Key Identifier;
- CRL Entry Extensions;
- Invalidity Date (UTC - optional); and
- Reason Code (optional).

7.3 OCSP Profile

No stipulation. Reserved for future use.

7.3.1 Version Number(s)

No stipulation. Reserved for future use.

7.3.2 OCSP Extensions

No stipulation. Reserved for future use.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

An annual audit is performed by an independent external auditor to assess Trustwave's compliance with the standards set forth by the CA/Browser Forum.

Material exceptions or deficiencies identified during an audit will result in a determination of actions to be taken. This determination is made by Trustwave management with input from the independent auditor. Trustwave management is responsible for developing and implementing a corrective action plan. Trustwave undergoes yearly audits using AICPA/CICA WebTrust for certification authorities, including extended validation criteria, for all components of the Trustwave managed TPH and complies with all requirements of the program.

8.1 Frequency or Circumstances of Assessment

Trustwave shall conduct the AICPA/CICA WebTrust audits on a yearly basis.

8.2 Identity/Qualifications of Assessor

The AICPA/CICA WebTrust audits shall be conducted by a certified public accounting firm with a sound foundation for conducting its audit business, that:

- Has no financial, business, or legal interest with Trustwave;
- Has demonstrated proficiency and competence in regards to public key infrastructure technology; and is
- Accredited by the American Institute of Certified Public Accountants (AICPA).

8.3 Assessor's Relationship to Assessed Entity

The public accounting firm conducts the AICPA/CICA WebTrust audits for Trustwave shall be completely independent of Trustwave.

8.4 Topics Covered by Assessment

The annual WebTrust audits shall include but are not limited to:

- CA business practices disclosure
- Detailed validation process
- Service integrity
- CA environmental controls.

8.5 Actions Taken as a Result of Deficiency

For any deficiencies found by the Web trust audit, Trustwave shall immediately develop a plan to implement remediation steps. This plan will be submitted to the Certification Practice Board and to the independent auditor within 30 days. Following acceptance of the plan, Trustwave shall immediately move to correct all deficiencies noted.

8.6 Communication of Results

All results of the WebTrust audit for Trustwave shall be communicated to the Certification Practice Board and to the Certification Operations Committee. Following review and approval by the Certification Practice Board, the results will be communicated to the Trustwave Board of Directors.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

Trustwave is entitled to charge Subscribers and End-Entities for the issuance, reissuance, management, rekey, and renewal of Certificates.

9.1.2 Certificate Access Fees

Trustwave may, in its discretion, charge a fee to make a Certificate available in a repository or available to a Relying Party.

9.1.3 Revocation or Status Information Access Fees

Trustwave may, in its discretion, charge a fee to view the CRL's and to make the CRL's available in a repository or to a Relying Party. Trustwave may also charge a fee to provide customized CRL's, OCSP services, or other value-added revocation status information services. Trustwave does not provide access to revocation information, Certificate status information, or time stamping in its repositories by third parties, including third parties that provide products and/or services that utilize such Certificate status information. Such access may, however, be provided with the prior written consent of Trustwave.

9.1.4 Fees for Other Services

Trustwave does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works is strictly prohibited without the express written consent of Trustwave.

9.1.5 Refund Policy

Trustwave's refund policy may be found at https://ssl.trustwave.com/CA.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

Trustwave encourages customer, Subscribers, End-Entities, Relying Parties, and all other entities to maintain adequate insurance to protect against errors and omissions, professional liability, and general liability. Trustwave currently maintains commercially reasonable insurance.

9.2.2 Other Assets

Customers shall maintain adequate financial resources for their operations and duties, and shall be able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Insurance or Warranty Coverage for End-Entities

Trustwave's warranty coverage for Relying Parties may be found at https://ssl.trustwave.com/CA.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following Subscriber documentation shall be maintained in confidence.

- CA application records, whether approved or disapproved;
- Certificate Application records;
- Subscriber Agreement
- Private keys held by customers and subscribers and information needed to recover such Private Keys;
- Transactional records;
- Contingency planning and disaster recovery plans; and
- Security measures controlling the operations of Trustwave' hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

This section is subject to applicable privacy laws. The following are not considered confidential:

- Certificates;
- Certificate revocation;
- Certificate status; and
- Trustwave repositories and their contents.

9.3.3 Responsibility to Protect Confidential Information

Trustwave protects and secures confidential information from disclosure.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

Trustwave's privacy plan/policy may be found at http://www.trustwave.com/legal.

9.4.2 Information Treated as Private

Non-public Subscriber information is treated as private.

9.4.3 Information Not Deemed Private

Subscriber information issued in the Certificates, Certificate directory, and online CRL's is not deemed private information, subject to applicable law.

9.4.4 Responsibility to Protect Private Information

Trustwave, customers, Subscribers, and End-Entities who receive private information shall protect it from disclosure to third parties and shall comply with all applicable laws.

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this CPS, Trustwave's Privacy Policy, or agreements in writing, private information shall not be used without the written consent of the party who owns such information. This section is subject to applicable laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Trustwave shall be permitted to disclose confidential and/or private information if Trustwave reasonably determines that disclosure is required in response to a subpoena, court order, search warrant, judicial, administrative, discovery, or other legal process or directive. This section is subject to applicable laws.

9.4.7 Other Information Disclosure Circumstances

Refer to section 9.4.6.

9.5 Intellectual Property Rights

Trustwave retains all rights, title, and interest, including without limitation intellectual property rights to the following:

- This CPS and CP's;
- Certificates;
- Revocation Information;
- Trustwave's logos, trademarks and service marks; and
- Trustwave's roots keys and the root Certificates containing them.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Trustwave warrants that, to the best of Trustwave's knowledge:

- there are no material misrepresentations of fact with the Certificates;
- there are no errors in the information within the Certificates caused by Trustwave's failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates;
- the Certificates comply with the material requirements of this CPS and the applicable CP's; and
- Trustwave's revocation services and its repositories materially comply with this CPS and the applicable CP's.

9.6.2 RA Representations and Warranties

RA's warrant that, to the best of their knowledge:

- there are no material misrepresentations of fact with the Certificates;
- there are no errors in the information within the Certificates caused by Trustwave's failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates;
- the Certificates comply with the material requirements of this CPS and the applicable CP's; and

- Trustwave's revocation services, if applicable, and its repositories materially comply with this CPS and the applicable CP's.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

- Each digital signature created using the private key corresponding to the public key listed in the Certificate is the digital signature of the Subscriber and the Certificate has been accepted and is operational (not expired or revoked) at the time the digital signature is created;
- Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key;
- All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
- All information supplied by the Subscriber and contained in the Certificate is true;
- The Certificate is being used exclusively for authorized and legal purposes consistent with this CPS, and
- The Subscriber is an end-user Subscriber and not a CA, and is not using the private key corresponding to any public key listed in the Certificate for purposes of digitally signing any Certificate (or any other format of certified public key) or CRL, as a CA or otherwise.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

Relying Party Agreements require Relying Parties to acknowledge that they have sufficient information to make an informed decision as to the extent to which they choose to rely on the information in a Certificate, that they are solely responsible for deciding whether or not to rely on such information, and that they shall bear the legal consequences and liability of their failure to perform the Relying Party obligations in terms of this CPS.

Relying Party Agreements may include additional representations and warranties.

9.7 Disclaimers of Warranties

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED HEREIN AND TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW, TRUSTWAVE EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH RESPECT TO THIS CPS, THE APPLICABLE CP'S OR ANY CERTIFICATE ISSUED HEREUNDER, INCLUDING WITHOUT LIMITATION, ALL WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE OR USE OF A CERTIFICATE OR ANY SERVICE (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) PROVIDED BY TRUSTWAVE AS DESCRIBED HEREIN. ALL WARRANTIES, REPRESENTATIONS, CONDITIONS, UNDERTAKINGS, TERMS AND OBLIGATIONS IMPLIED BY STATUTE OR COMMON LAW, TRADE USAGE, COURSE OF DEALING OR OTHERWISE ARE HEREBY EXCLUDED TO THE FULLEST EXTENT PERMITTED BY LAW. EXCEPT FOR THE LIMITED WARRANTY DESCRIBED HEREIN, TRUSTWAVE FURTHER DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, TO ANY APPLICANT, SUBSCRIBER OR ANY RELYING PARTY THAT (1) THE

SUBSCRIBER TO WHICH IT HAS ISSUED A CERTIFICATE IS IN THE FACT THE PERSON, ENTITY OR ORGANIZATION IT CLAIMS TO HAVE BEEN (2) A SUBSCRIBER IS IN FACT THE PERSON, ENTITY OR ORGANIZATION LISTED IN THE CERTIFICATE, OR (3) THAT THE INFORMATION CONTAINED IN THE CERTIFICATES OR IN ANY CERTIFICATE STATUS MECHANISM COMPILED, PUBLISHED OR OTHERWISE DISSEMINATED BY TRUSTWAVE, OR THE RESULTS OF ANY CRYPTOGRAPHIC METHOD IMPLEMENTED IN CONNECTION WITH THE CERTIFICATES IS ACCURATE, AUTHENTIC, COMPLETE OR RELIABLE.

IT IS AGREED AND ACKNOWLEDGED THAT APPLICANTS AND SUBSCRIBERS ARE LIABLE FOR ANY MISREPRESENTATIONS MADE TO TRUSTWAVE OR RELIED UPON BY A RELYING PARTY. TRUSTWAVE DOES NOT WARRANT OR GUARANTEE UNDER ANY CIRCUMSTANCES THE "NON-REPUDIATION" BY A SUBSCRIBER AND/OR RELYING PARTY OF ANY TRANSACTION OR CONTRACT ENTERED INTO BY THE SUBSCRIBER AND/OR RELYING PARTY INVOLVING THE USE OF OR RELIANCE UPON A CERTIFICATE.

IT IS UNDERSTOOD AND AGREED UPON BY SUBSCRIBERS AND RELYING PARTIES THAT IN USING AND/OR RELYING UPON A CERTIFICATE THEY ARE SOLELY RESPONSIBLE FOR THEIR RELIANCE UPON THAT CERTIFICATE AND THAT SUCH PARTIES MUST CONSIDER THE FACTS, CIRCUMSTANCES AND CONTEXT SURROUNDING THE TRANSACTION IN WHICH THE CERTIFICATE IS USED IN DETERMINING SUCH RELIANCE.

THE APPLICANTS, SUBSCRIBERS AND RELYING PARTIES AGREE AND ACKNOWLEDGE THAT CERTIFICATES HAVE A LIMITED VALIDITY PERIOD AND MAY BE REVOKED AT ANY TIME. SUBSCRIBERS AND RELYING PARTIES ARE UNDER AN OBLIGATION TO VERIFY WHETHER A CERTIFICATE IS EXPIRED OR HAS BEEN REVOKED. TRUSTWAVE HEREBY DISCLAIMS ANY AND ALL LIABILITY TO SUBSCRIBERS AND RELYING PARTIES WHO DO NOT FOLLOW SUCH PROCEDURES, THIS CPS, OR THE APPLICABLE CP'S.

Trustwave provides no warranties with respect to another party's software, hardware, telecommunications or networking equipment utilized in connection with the use, issuance, revocation or management of Certificates or providing other services (including, without limitation, any support services) with respect to this CPS or the applicable CP's. Applicants, Subscribers and Relying Parties agree and acknowledge that Trustwave is not responsible or liable for any misrepresentations or incomplete representations of Certificates or any information contained therein caused by another party's application software or graphical user interfaces. The cryptographic key-generation technology used by Applicants, Subscribers and Relying Parties in conjunction with the Certificates may or may not be subject to the intellectual property rights of third-parties. It is the responsibility of Applicants, Subscribers and Relying Parties to ensure that they are using technology which is properly licensed or to otherwise obtain the right to use such technology

9.8 Limitations of Liability

IN NO EVENT SHALL THE CUMULATIVE OR AGGREGATE LIABILITY OF TRUSTWAVE TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY FOR ALL CLAIMS RELATED TO THE INSTALLATION OF, USE OF OR RELIANCE UPON A

SPECIFIC CERTIFICATE INCLUDING WITHOUT LIMITATION ANY CAUSE OF ACTION OR CLAIM IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND TORTIOUS INTERFERENCE WITH CONTRACT), STRICT LIABILITY, FOR BREACH OF A STATUTORY DUTY OR FIDUCIARY DUTY OR IN ANY OTHER WAY, EXCEED TWO THOUSAND U.S. DOLLARS ($2,000.00 USD). THE FOREGOING LIMITATIONS OF LIABILITY SHALL APPLY ON A CERTIFICATE-BY-CERTIFICATE BASIS, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CLAIMS RELATED TO EACH CERTIFICATE, AND SHALL BE APPORTIONED FIRST TO THE EARLIER CLAIMS TO ACHIEVE FINAL RESOLUTION.

TRUSTWAVE SHALL NOT BE LIABLE IN CONTRACT, TORT (INCLUDING NEGLIGENCE AND TORTIOUS INTERFERENCE WITH CONTRACT), STRICT LIABILITY, FOR BREACH OF A STATUTORY OR FIDUCIARY DUTY OR IN ANY OTHER WAY (EVEN IF FORSEEABLE AND/OR TRUSTWAVE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES) FOR: (I) ANY ECONOMIC LOSS (INCLUDING, WITHOUT LIMITATION, LOSS OF REVENUES, PROFITS, CONTRACTS, BUSINESS OR ANTICIPATED SAVINGS); (II) TO THE EXTENT ALLOWED BY APPLICABLE LAW, ANY LOSS OR DAMAGE RESULTING FROM DEATH OR INJURY OF SUBSCRIBER AND/OR ANY RELYING PARTY OR ANYONE ELSE; (III) NON-ECONOMIC LOSS OR ANY LOSS OF GOODWILL OR REPUTATION; OR (IV) ANY OTHER INDIRECT, CONSEQUENTIAL, INCIDENTAL, MULTIPLE, SPECIAL, PUNITIVE, EXEMPLARY DAMAGES.

THIS SECTION “LIMITATIONS OF LIABILITY” SHALL APPLY WHETHER OR NOT SUCH LOSSES OR DAMAGES WERE WITHIN THE CONTEMPLATION OF THE PARTIES AT THE TIME OF THE APPLICATION FOR, INSTALLATION, USE, OR’ RELIANCE ON THE CERTIFICATE, OR AROSE OUT OF ANY OTHER MATTER OR SERVICES (INCLUDING, WITHOUT LIMITATION, ANY SUPPORT SERVICES) UNDER THIS CPS OR THE APPLICABLE CP’S OR WITH REGARD TO THE USE OF OR RELIANCE ON THE CERTIFICATE.

IN THE EVENT THAT SOME JURISDICTIONS DO NOT PERMIT THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, THE ABOVE EXCLUSIONS OF INCIDENTAL AND CONSEQUENTIAL DAMAGES MAY NOT APPLY TO AN APPLICANT, SUBSCRIBER AND/OR A RELYING PARTY BUT SHALL BE GIVEN EFFECT TO THE FULLEST AND GREATEST EXTENT PERMITTED BY APPLICABLE LAW.

In no event will Trustwave be liable for any damages to Applicants, Subscribers, Relying Parties or any other party arising out of or related to the use or misuse of, or reliance on any Certificate issued under this CPS that: (i) has expired or been revoked; (ii) has been used for any purpose other than as set forth in the CPS; (iii) has been tampered with; (iv) has been Compromised or if the Key Pair underlying such Certificate or the cryptography algorithm used to generate such Certificate's Key Pair, has been Compromised by the action of any party other than Trustwave (including without limitation the Applicant, Subscriber or Relying Party); or (v) is the subject of misrepresentations or other misleading acts or omissions of any other party, including but not limited to Applicants, Subscribers and Relying Parties. In no event shall Trustwave be liable to the Applicant, Subscriber, Relying Party or other party for damages arising out of any claim that a Certificate infringes any patent, trademark, copyright, trade secret or other intellectual property right of any party.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber agreements.

The liability (and/or limitation thereof) of enterprise RAs and the applicable CA shall be set out in the agreement(s) between them.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 Indemnities

Applicant, Subscriber and Relying Parties hereby agree to indemnify and hold Trustwave and its affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partner, successors and assigns) harmless from any claims, actions, or demands that are caused by the use, publication or reliance on a Certificate and that arises from (a) any false or misleading statement of fact by the Applicant (or any person acting on the behalf of the Applicant) (b) any failure by the Applicant or the Subscriber to disclose a material fact, regardless of whether such omission was made negligently or with the intent to deceive; (c) any failure on the part of the Subscriber to protect its Private Key and Certificate or to take the precautions necessary to prevent the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate; (d) any failure on the part of the Subscriber to promptly notify Trustwave, as the case may be, of the Compromise, disclosure, loss, modification or unauthorized use of the Private Key or Certificate once the Subscriber has constructive or actual notice of such event; (e) the Subscriber's failure to the comply with the Subscriber Agreement; or (f) the Relying Party's failure to comply with this CPS and the Relying Party Agreement, including without limitation the Relying Party's (i) failure to verify a Certificate in accordance with this CPS and the Relying Party Agreement; (ii) reliance on a Certificate that is unreasonable given the circumstances; and/or (iii) failure to verify whether a Certificate has expired or been revoked.

The applicable Subscriber and/or Relying Party Agreements may set forth additional indemnity obligations.

9.10 Term and Termination

9.10.1 Term

This CPS and the CP's, and any amendments thereto, are effective upon publication in Trustwave's Repository.

9.10.2 Termination

This CPS and the CP's, as may be amended from time to time, are effective until replace by a new version, which shall be published in Trustwave's Repository.

9.10.3 Effect of Termination and Survival

Upon Termination of this CPS or the applicable CP's, customers, Subscribers, and Relying Parties are bound by its terms for all Certificates issued, while it's effective, for the remainder of the validity periods of such Certificates.

9.11 Individual Notices and Communications with Participants

Trustwave, Subscribers, Applicants, Relying Parties and other participants will use commercially reasonable methods to communicate with each other.

9.12 Amendments

9.12.1 Procedure for Amendment

Refer to Section 1.5.4 hereof.

9.12.2 Notification Mechanism and Period

Trustwave reserves the right to amend this CPS and the applicable CP's without notification for amendments that are not material. Trustwave's decision to designate an amendment's materiality shall be within the sole discretion of Trustwave's Certification Practice Board.

Updates, amendments, and new version of Trustwave's CPS and the applicable CP's shall be posted in Trustwave's repository. Such publication shall serve as notice to all relevant entities.

9.12.3 Circumstances under Which OID Must be Changed

If Trustwave's Certification Practice Board determines that a change is necessary in the object identifier corresponding to a Certificate policy, the amendment shall contain new object identifiers for the Certificate policies corresponding to each such Certificate. Otherwise, amendments shall not require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

Any dispute, controversy or claim, which cannot be mutually resolved within ninety (90) days, arising under, in connection with or relating to this CPS the applicable CP's, Trustwave's Websites, or any Certificate issued by Trustwave shall be subject to and settled finally by binding arbitration in accordance with the Arbitration Rules of the American Arbitration Association (AAA). All arbitration proceedings shall be held in Chicago, Illinois. There shall be one arbitrator appointed by the AAA who shall exhibit a reasonable familiarity with the issues involved or presented in such dispute, controversy or claim. The award of the arbitrator shall be binding and final upon all parties, and judgment on the award may be entered by any court having proper jurisdiction thereof. This CPS, the applicable CP's and the rights and obligations of the parties hereunder and under any Certificate issued by Trustwave shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys fees actually incurred.

9.14 Governing Law

The enforceability, construction, interpretation, and validity of this CPS, the applicable CP's and any Certificates issued by Trustwave shall be governed by the substantive laws of the State of Delaware, United States of America, excluding (i) the conflicts of law provisions thereof and (ii) the United Nations Convention on Contracts for the International Sale of Goods. Applicants, Subscribers, and Relying Parties irrevocably consent to jurisdiction in

the State of Illinois and any and all actions against Trustwave or its affiliated companies shall be brought in the State of Illinois.

9.15 Compliance with Applicable Law

This CPS and the applicable CP's is subject to applicable federal, state, local and foreign laws, rules, regulations including, but not limited to, restrictions on exporting or importing software, hardware, or information

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

This CPS, the applicable CP's, and the applicable Subscriber Agreement and Relying Party Agreement represent the entire agreement between any Subscriber or Relying Party and Trustwave and shall supersede any and all prior understandings and representations pertaining to its subject matter. In the event, however, of a conflict between this CPS and any other express agreement between a Subscriber or Relying Party with Trustwave with respect to a Certificate, including but not limited to a Subscriber Agreement, and Relying Party such other agreement shall take precedence.

9.16.2 Assignment

This CPS and its CP's shall not be assigned to any party without the express prior written consent of Trustwave's Legal Department.

9.16.3 Severability

If any provision of this CPS and/or the CP's shall be held to be invalid, illegal, or unenforceable, the validity, legality, or enforceability of the remainder of this CPS and the CP's shall remain in full force and effect.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

The waiver or failure to exercise any right provided for in this CPS or the applicable CP's shall not be deemed a waiver of any further or future right under this CPS or the applicable CP's.

9.16.5 Force Majeure

Trustwave shall not be liable for any default or delay in the performance of its obligations hereunder to the extent and while such default or delay is caused, directly or indirectly, by fire, flood, earthquake, elements of nature or acts of God, acts of war, terrorism, riots, civil disorders, rebellions or revolutions, strikes, lockouts, or labor difficulties or any other similar cause beyond the reasonable control of Trustwave.

9.17 Other Provisions

No stipulation.

10. Appendix A –

Trustwave Global Root Certificates

10.1 XGCA - XRamp Global Certification Authority -

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            50:94:6c:ec:18:ea:d5:9c:4d:d5:97:ef:75:8f:a0:ad
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, OU=www.xrampsecurity.com, O=XRamp Security Services
Inc,
CN=XRamp Global Certification Authority
        Validity
            Not Before: Nov  1 17:14:04 2004 GMT
            Not After : Jan  1 05:37:19 2035 GMT
        Subject: C=US, OU=www.xrampsecurity.com, O=XRamp Security Services
Inc,
CN=XRamp Global Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:98:24:1e:bd:15:b4:ba:df:c7:8c:a5:27:b6:38:
                    0b:69:f3:b6:4e:a8:2c:2e:21:1d:5c:44:df:21:5d:
                    7e:23:74:fe:5e:7e:b4:4a:b7:a6:ad:1f:ae:e0:06:
                    16:e2:9b:5b:d9:67:74:6b:5d:80:8f:29:9d:86:1b:
                    d9:9c:0d:98:6d:76:10:28:58:e4:65:b0:7f:4a:98:
                    79:9f:e0:c3:31:7e:80:2b:b5:8c:c0:40:3b:11:86:
                    d0:cb:a2:86:36:60:a4:d5:30:82:6d:d9:6e:d0:0f:
                    12:04:33:97:5f:4f:61:5a:f0:e4:f9:91:ab:e7:1d:
                    3b:bc:e8:cf:f4:6b:2d:34:7c:e2:48:61:1c:8e:f3:
                    61:44:cc:6f:a0:4a:a9:94:b0:4d:da:e7:a9:34:7a:
                    72:38:a8:41:cc:3c:94:11:7d:eb:c8:a6:8c:b7:86:
                    cb:ca:33:3b:d9:3d:37:8b:fb:7a:3e:86:2c:e7:73:
                    d7:0a:57:ac:64:9b:19:eb:f4:0f:04:08:8a:ac:03:
                    17:19:64:f4:5a:25:22:8d:34:2c:b2:f6:68:1d:12:
                    6d:d3:8a:1e:14:da:c4:8f:a6:e2:23:85:d5:7a:0d:
                    bd:6a:e0:e9:ec:ec:17:bb:42:1b:67:aa:25:ed:45:
                    83:21:fc:c1:c9:7c:d5:62:3e:fa:f2:c5:2d:d3:fd:
                    d4:65
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage:
            Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
            CA:TRUE
            X509v3 Subject Key Identifier:
            C6:4F:A2:3D:06:63:84:09:9C:CE:62:E4:04:AC:8D:5C:B5:E9:B6:1B
            X509v3 CRL Distribution Points:
            URI:http://crl.xrampsecurity.com/XGCA.crl
```

```
            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        91:15:39:03:01:1b:67:fb:4a:1c:f9:0a:60:5b:a1:da:4d:97:
        62:f9:24:53:27:d7:82:64:4e:90:2e:c3:49:1b:2b:9a:dc:fc:
        a8:78:67:35:f1:1d:f0:11:bd:b7:48:e3:10:f6:0d:df:3f:d2:
        c9:b6:aa:55:a4:48:ba:02:db:de:59:2e:15:5b:3b:9d:16:7d:
        47:d7:37:ea:5f:4d:76:12:36:bb:1f:d7:a1:81:04:46:20:a3:
        2c:6d:a9:9e:01:7e:3f:29:ce:00:93:df:fd:c9:92:73:89:89:
        64:9e:e7:2b:e4:1c:91:2c:d2:b9:ce:7d:ce:6f:31:99:d3:e6:
        be:d2:1e:90:f0:09:14:79:5c:23:ab:4d:d2:da:21:1f:4d:99:
        79:9d:e1:cf:27:9f:10:9b:1c:88:0d:b0:8a:64:41:31:b8:0e:
        6c:90:24:a4:9b:5c:71:8f:ba:bb:7e:1c:1b:db:6a:80:0f:21:
        bc:e9:db:a6:b7:40:f4:b2:8b:a9:b1:e4:ef:9a:1a:d0:3d:69:
        99:ee:a8:28:a3:e1:3c:b3:f0:b2:11:9c:cf:7c:40:e6:dd:e7:
        43:7d:a2:d8:3a:b5:a9:8d:f2:34:99:c4:d4:10:e1:06:fd:09:
        84:10:3b:ee:c4:4c:f4:ec:27:7c:42:c2:74:7c:82:8a:09:c9:
        b4:03:25:bc

-----BEGIN CERTIFICATE-----
MIIEMDCCAxigAwIBAgIQUJRs7Bjq1ZxN1ZfvdY+grTANBgkqhkiG9w0BAQUFADCB
gjELMAkGA1UEBhMCVVMxHjAcBgNVBAsTFXd3dy54cmFtcHNlY3VyaXR5LmNvbTEk
MCIGA1UEChMbWFJhbXAgU2VjdXJpdHkgU2VydmljZXMgSW5jMS0wKwYDVQQDEyRY
UmFtcCBHbG9iYWwgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwHhcNMDQxMTAxMTcx
NDA0WhcNMzUwMTAxMDUzNzE5WjCBgjELMAkGA1UEBhMCVVMxHjAcBgNVBAsTFXd3
dy54cmFtcHNlY3VyaXR5LmNvbTEkMCIGA1UEChMbWFJhbXAgU2VjdXJpdHkgU2Vy
dmljZXMgSW5jMS0wKwYDVQQDEyRYUmFtcCBHbG9iYWwgQ2VydGlmaWNhdGlvbiBB
dXRob3JpdHkwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCYJB69FbS6
38eMpSe2OAtp87ZOqCwuIR1cRN8hXX4jdP5efrRKt6atH67gBhbim1vZZ3RrXYCP
KZ2GG9mcDZhtdhAoWORlsH9KmHmf4MMxfoArtYzAQDsRhtDLooY2YKTVMIJt2W7Q
DxIEM5dfT2Fa8OT5kavnHTu86M/0ay00fOJIYRyO82FEzG+gSqmUsE3a56k0enI4
qEHMPJQRfevIpoy3hsvKMzvZPTeL+3o+hiznc9cKV6xkmxnr9A8ECIqsAxcZZPRa
JSKNNCyy9mgdEm3Tih4U2sSPpuIjhdV6Db1q4Ons7Be7QhtnqiXtRYMh/MHJfNVi
PvryxS3T/dRlAgMBAAGjgZ8wgZwwEwYJKwYBBAGCNxQCBAYeBABDAEEwCwYDVR0P
BAQDAgGGMA8GA1UdEwEB/wQFMAMBAf8wHQYDVR0OBBYEFMZPoj0GY4QJnM5i5ASs
jVy16bYbMDYGA1UdHwQvMC0wK6ApoCeGJWh0dHA6Ly9jcmwueHJhbXBzZWN1cml0
eS5jb20vWEdDQS5jcmwwEAYJKwYBBAGCNxUBBAMCAQEwDQYJKoZIhvcNAQEFBQAD
ggEBAJEVOQMBG2f7Shz5CmBbodpNl2L5JFMn14JkTpAuw0kbK5rc/Kh4ZzXxHfAR
vbdI4xD2Dd8/0sm2qlWkSLoC295ZLhVbO50WfUfXN+pfTXYSNrsf16GBBEYgoyxt
qZ4Bfj8pzgCT3/3JknOJiWSe5yvkHJEs0rnOfc5vMZnT5r7SHpDwCRR5XCOrTdLa
IR9NmXmd4c8nnxCbHIgNsIpkQTG4DmyQJKSbXHGPurt+HBvbaoAPIbzp26a3QPSy
i6mx5O+aGtA9aZnuqCij4Tyz8LIRnM98QObd50N9otg6tamN8jSZxNQQ4Qb9CYQQ
O+7ETPTsJ3xCwnR8gooJybQDJbw=
-----END CERTIFICATE-----
```

10.2 SGCA - Trustwave Secure Global CA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            07:56:22:a4:e8:d4:8a:89:4d:f4:13:c8:f0:f8:ea:a5
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=SecureTrust Corporation, CN=Secure Global CA
        Validity
            Not Before: Nov  7 19:42:28 2006 GMT
            Not After : Dec 31 19:52:06 2029 GMT
```

```
        Subject: C=US, O=SecureTrust Corporation, CN=Secure Global CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:af:35:2e:d8:ac:6c:55:69:06:71:e5:13:68:24:
                    b3:4f:d8:cc:21:47:f8:f1:60:38:89:89:03:e9:bd:
                    ea:5e:46:53:09:dc:5c:f5:5a:e8:f7:45:2a:02:eb:
                    31:61:d7:29:33:4c:ce:c7:7c:0a:37:7e:0f:ba:32:
                    98:e1:1d:97:af:8f:c7:dc:c9:38:96:f3:db:1a:fc:
                    51:ed:68:c6:d0:6e:a4:7c:24:d1:ae:42:c8:96:50:
                    63:2e:e0:fe:75:fe:98:a7:5f:49:2e:95:e3:39:33:
                    64:8e:1e:a4:5f:90:d2:67:3c:b2:d9:fe:41:b9:55:
                    a7:09:8e:72:05:1e:8b:dd:44:85:82:42:d0:49:c0:
                    1d:60:f0:d1:17:2c:95:eb:f6:a5:c1:92:a3:c5:c2:
                    a7:08:60:0d:60:04:10:96:79:9e:16:34:e6:a9:b6:
                    fa:25:45:39:c8:1e:65:f9:93:f5:aa:f1:52:dc:99:
                    98:3d:a5:86:1a:0c:35:33:fa:4b:a5:04:06:15:1c:
                    31:80:ef:aa:18:6b:c2:7b:d7:da:ce:f9:33:20:d5:
                    f5:bd:6a:33:2d:81:04:fb:b0:5c:d4:9c:a3:e2:5c:
                    1d:e3:a9:42:75:5e:7b:d4:77:ef:39:54:ba:c9:0a:
                    18:1b:12:99:49:2f:88:4b:fd:50:62:d1:73:e7:8f:
                    7a:43
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage:
            Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
            CA:TRUE
            X509v3 Subject Key Identifier:
            AF:44:04:C2:41:7E:48:83:DB:4E:39:02:EC:EC:84:7A:E6:CE:C9:A4
            X509v3 CRL Distribution Points:
            URI:http://crl.securetrust.com/SGCA.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        63:1a:08:40:7d:a4:5e:53:0d:77:d8:7a:ae:1f:0d:0b:51:16:
        03:ef:18:7c:c8:e3:af:6a:58:93:14:60:91:b2:84:dc:88:4e:
        be:39:8a:3a:f3:e6:82:89:5d:01:37:b3:ab:24:a4:15:0e:92:
        35:5a:4a:44:5e:4e:57:fa:75:ce:1f:48:ce:66:f4:3c:40:26:
        92:98:6c:1b:ee:24:46:0c:17:b3:52:a5:db:a5:91:91:cf:37:
        d3:6f:e7:27:08:3a:4e:19:1f:3a:a7:58:5c:17:cf:79:3f:8b:
        e4:a7:d3:26:23:9d:26:0f:58:69:fc:47:7e:b2:d0:8d:8b:93:
        bf:29:4f:43:69:74:76:67:4b:cf:07:8c:e6:02:f7:b5:e1:b4:
        43:b5:4b:2d:14:9f:f9:dc:26:0d:bf:a6:47:74:06:d8:88:d1:
        3a:29:30:84:ce:d2:39:80:62:1b:a8:c7:57:49:bc:6a:55:51:
        67:15:4a:be:35:07:e4:d5:75:98:37:79:30:14:db:29:9d:6c:
        c5:69:cc:47:55:a2:30:f7:cc:5c:7f:c2:c3:98:1c:6b:4e:16:
        80:eb:7a:78:65:45:a2:00:1a:af:0c:0d:55:64:34:48:b8:92:
        b9:f1:b4:50:29:f2:4f:23:1f:da:6c:ac:1f:44:e1:dd:23:78:
        51:5b:c7:16

-----BEGIN CERTIFICATE-----
MIIDvDCCAqSgAwIBAgIQB1YipOjUiolN9BPI8PjqpTANBgkqhkiG9w0BAQUFADBK
```

```
MQswCQYDVQQGEwJVUzEgMB4GA1UEChMXU2VjdXJlVHJ1c3QgQ29ycG9yYXRpb24x
GTAXBgNVBAMTEFNlY3VyZSBHbG9iYWwgQ0EwHhcNMDYxMTA3MTk0MjI4WhcNMjkx
MjMxMTk1MjA2WjBKMQswCQYDVQQGEwJVUzEgMB4GA1UEChMXU2VjdXJlVHJ1c3Qg
Q29ycG9yYXRpb24xGTAXBgNVBAMTEFNlY3VyZSBHbG9iYWwgQ0EwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCvNS7YrGxVaQZx5RNoJLNP2MwhR/jxYDiJ
iQPpvepeRlMJ3Fz1Wuj3RSoC6zFh1ykzTM7HfAo3fg+6MpjhHZevj8fcyTiW89sa
/FHtaMbQbqR8JNGuQsiWUGMu4P51/pinX0kuleM5M2SOHqRfkNJnPLLZ/kG5VacJ
jnIFHovdRIWCQtBJwB1g8NEXLJXr9qXBkqPFwqcIYA1gBBCWeZ4WNOaptvolRTnI
HmX5k/Wq8VLcmZg9pYYaDDUz+kulBAYVHDGA76oYa8J719rO+TMg1fW9ajMtgQT7
sFzUnKPiXB3jqUJ1XnvUd+85VLrJChgbEplJL4hL/VBi0XPnj3pDAgMBAAGjgZ0w
gZowEwYJKwYBBAGCNxQCBAYeBABDAEEwCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQF
MAMBAf8wHQYDVR0OBBYEFK9EBMJBfkiD2045AuzshHrmzsmkMDQGA1UdHwQtMCsw
KaAnoCWGI2h0dHA6Ly9jcmwuc2VjdXJldHJ1c3QuY29tL1NHQ0EuY3JsMBAGCSsG
AQQBgjcVAQQDAgEAMA0GCSqGSIb3DQEBBQUAA4IBAQBjGghAfaReUw132HquHw0L
URYD7xh8yOOvaliTFGCRsoTciE6+OYo68+aCiV0BN7OrJKQVDpI1WkpEXk5X+nXO
H0jOZvQ8QCaSmGwb7iRGDBezUqXbpZGRzzfTb+cnCDpOGR86p1hcF895P4vkp9Mm
I50mD1hp/Ed+stCNi5O/KU9DaXR2Z0vPB4zmAve14bRDtUstFJ/53CYNv6ZHdAbY
iNE6KTCEztI5gGIbqMdXSbxqVVFnFUq+NQfk1XWYN3kwFNspnWzFacxHVaIw98xc
f8LDmBxrThaA63p4ZUWiABqvDA1VZDRIuJK58bRQKfJPIx/abKwfROHdI3hRW8cW
-----END CERTIFICATE-----
```

NEED PARSE

10.3 STCA - Trustwave SecureTrust CA

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0c:f0:8e:5c:08:16:a5:ad:42:7f:f0:eb:27:18:59:d0
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=SecureTrust Corporation, CN=SecureTrust CA
        Validity
            Not Before: Nov  7 19:31:18 2006 GMT
            Not After : Dec 31 19:40:55 2029 GMT
        Subject: C=US, O=SecureTrust Corporation, CN=SecureTrust CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:ab:a4:81:e5:95:cd:f5:f6:14:8e:c2:4f:ca:d4:
                    e2:78:95:58:9c:41:e1:0d:99:40:24:17:39:91:33:
                    66:e9:be:e1:83:af:62:5c:89:d1:fc:24:5b:61:b3:
                    e0:11:11:41:1c:1d:6e:f0:b8:bb:f8:de:a7:81:ba:
                    a6:48:c6:9f:1d:bd:be:8e:a9:41:3e:b8:94:ed:29:
                    1a:d4:8e:d2:03:1d:03:ef:6d:0d:67:1c:57:d7:06:
                    ad:ca:c8:f5:fe:0e:af:66:25:48:04:96:0b:5d:a3:
                    ba:16:c3:08:4f:d1:46:f8:14:5c:f2:c8:5e:01:99:
                    6d:fd:88:cc:86:a8:c1:6f:31:42:6c:52:3e:68:cb:
                    f3:19:34:df:bb:87:18:56:80:26:c4:d0:dc:c0:6f:
                    df:de:a0:c2:91:16:a0:64:11:4b:44:bc:1e:f6:e7:
                    fa:63:de:66:ac:76:a4:71:a3:ec:36:94:68:7a:77:
                    a4:b1:e7:0e:2f:81:7a:e2:b5:72:86:ef:a2:6b:8b:
                    f0:0f:db:d3:59:3f:ba:72:bc:44:24:9c:e3:73:b3:
                    f7:af:57:2f:42:26:9d:a9:74:ba:00:52:f2:4b:cd:
                    53:7c:47:0b:36:85:0e:66:a9:08:97:16:34:57:c1:
                    66:f7:80:e3:ed:70:54:c7:93:e0:2e:28:15:59:87:
                    ba:bb
                Exponent: 65537 (0x10001)
```

```
        X509v3 extensions:
            1.3.6.1.4.1.311.20.2:
                ...C.A
            X509v3 Key Usage:
            Digital Signature, Certificate Sign, CRL Sign
            X509v3 Basic Constraints: critical
            CA:TRUE
            X509v3 Subject Key Identifier:
            42:32:B6:16:FA:04:FD:FE:5D:4B:7A:C3:FD:F7:4C:40:1D:5A:43:AF
            X509v3 CRL Distribution Points:
            URI:http://crl.securetrust.com/STCA.crl

            1.3.6.1.4.1.311.21.1:
                ...
    Signature Algorithm: sha1WithRSAEncryption
        30:ed:4f:4a:e1:58:3a:52:72:5b:b5:a6:a3:65:18:a6:bb:51:
        3b:77:e9:9d:ea:d3:9f:5c:e0:45:65:7b:0d:ca:5b:e2:70:50:
        b2:94:05:14:ae:49:c7:8d:41:07:12:73:94:7e:0c:23:21:fd:
        bc:10:7f:60:10:5a:72:f5:98:0e:ac:ec:b9:7f:dd:7a:6f:5d:
        d3:1c:f4:ff:88:05:69:42:a9:05:71:c8:b7:ac:26:e8:2e:b4:
        8c:6a:ff:71:dc:b8:b1:df:99:bc:7c:21:54:2b:e4:58:a2:bb:
        57:29:ae:9e:a9:a3:19:26:0f:99:2e:08:b0:ef:fd:69:cf:99:
        1a:09:8d:e3:a7:9f:2b:c9:36:34:7b:24:b3:78:4c:95:17:a4:
        06:26:1e:b6:64:52:36:5f:60:67:d9:9c:c5:05:74:0b:e7:67:
        23:d2:08:fc:88:e9:ae:8b:7f:e1:30:f4:37:7e:fd:c6:32:da:
        2d:9e:44:30:30:6c:ee:07:de:d2:34:fc:d2:ff:40:f6:4b:f4:
        66:46:06:54:a6:f2:32:0a:63:26:30:6b:9b:d1:dc:8b:47:ba:
        e1:b9:d5:62:d0:a2:a0:f4:67:05:78:29:63:1a:6f:04:d6:f8:
        c6:4c:a3:9a:b1:37:b4:8d:e5:28:4b:1d:9e:2c:c2:b8:68:bc:
        ed:02:ee:31
```

```
-----BEGIN CERTIFICATE-----
MIIDuDCCAqCgAwIBAgIQDPCOXAgWpa1Cf/DrJxhZ0DANBgkqhkiG9w0BAQUFADBI
MQswCQYDVQQGEwJVUzEgMB4GA1UEChMXU2VjdXJlVHJ1c3QgQ29ycG9yYXRpb24x
FzAVBgNVBAMTDlNlY3VyZVRydXN0IENBMB4XDTA2MTEwNzE5MzExOFoXDTI5MTIz
MTE5NDA1NVowSDELMAkGA1UEBhMCVVMxIDAeBgNVBAoTF1NlY3VyZVRydXN0IENv
cnBvcmF0aW9uMRcwFQYDVQQDEw5TZWN1cmVUcnVzdCBDQTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBAKukgeWVzfX2FI7CT8rU4niVWJxB4Q2ZQCQXOZEz
Zum+4YOvYlyJ0fwkW2Gz4BERQRwdbvC4u/jep4G6pkjGnx29vo6pQT64lO0pGtSO
0gMdA+9tDWccV9cGrcrI9f4Or2YlSASWC12juhbDCE/RRvgUXPLIXgGZbf2IzIao
wW8xQmxSPmjL8xk037uHGFaAJsTQ3MBv396gwpEWoGQRS0S8Hvbn+mPeZqx2pHGj
7DaUaHp3pLHnDi+BeuK1cobvomuL8A/b01k/unK8RCSc43Oz969XL0Imnal0ugBS
8kvNU3xHCzaFDmapCJcWNFfBZveA4+1wVMeT4C4oFVmHursCAwEAAaOBnTCBmjAT
BgkrBgEEAYI3FAIEBh4EAEMAQTALBgNVHQ8EBAMCAYYwDwYDVR0TAQH/BAUwAwEB
/zAdBgNVHQ4EFgQUQjK2FvoE/f5dS3rD/fdMQB1aQ68wNAYDVR0fBC0wKzApoCeg
JYYjaHR0cDovL2NybC5zZWN1cmV0cnVzdC5jb20vU1RDQS5jcmwwEAYJKwYBBAGC
NxUBBAMCAQAwDQYJKoZIhvcNAQEFBQADggEBADDtT0rhWDpSclu1pqNlGKa7UTt3
6Z3q059c4EVlew3KW+JwULKUBRSuSceNQQcSc5R+DCMh/bwQf2AQWnL1mA6s7Ll/
3XpvXdMc9P+IBWlCqQVxyLesJugutIxq/3HcuLHfmbx8IVQr5Fiiu1cprp6poxkm
D5kuCLDv/WnPmRoJjeOnnyvJNjR7JLN4TJUXpAYmHrZkUjZfYGfZnMUFdAvnZyPS
CPyI6a6Lf+Ew9Dd+/cYy2i2eRDAwbO4H3tI0/NL/QPZL9GZGBlSm8jIKYyYwa5vR
3ItHuuG51WLQoqD0ZwV4KWMabwTW+MZMo5qxN7SN5ShLHZ4swrhovO0C7jE=
-----END CERTIFICATE-----
```