# Trustwave Holdings, Inc

## Certificate Policy and Certification Practices Statement

Version 2.9

Effective Date: July 13, 2010

This document contains Certification Practices and Certificate Policies applicable to identifiers beginning with:

- 1.3.6.1.4.1.30360.3.3.3, and
- 2.16.840.1.114404

This document defines “Certification Practice” and “Certificate Policy” for all Trustwave Holdings (hereinafter, "Trustwave") Certification Authorities and Digital Certificates. All Digital Certificates that have been issued by Trustwave shall contain one of the following identifiers within the "certificatePolicies extension" field in the Digital Certificate. This document contains all Certificate Policies and the Certification Practices for the Trustwave Certification Authority that issued the Digital Certificate which contains one of the following Certificate Policy identifiers.

| | Certificate Type | Friendly Name | Certificate Policy ID |
|---|---|---|---|
| 1. | Email S/MIME Digital Certificate | S/MIME Certificate, Secure E-Mail Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.5.4.3.3 |
| 2. | Organization Validation (“OV”) Code Signing Certificate | OV Code Signing Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.3.4 |
| 3. | Special Use Certificate | SUCA Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.5.3 |
| 4. | Independent Organization Certification Authority Certificate | ORGCA Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.4.4.4.3 |
| 5. | Client Authentication Certificate | Client Authentication Certificate, "My Identity" Certificate, VPN Certificate | 1.3.6.1.4.1.30360.3.3.3.5.4.6.3<br>1.3.6.1.4.1.30360.3.3.3.4.4.6.3 |
| 6. | Internal SSL Certificate | ISSL Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.7.3 |
| 7. | Extended Validation (“EV”) Web Server SSL Digital Certificate | EV Certificate | 2.16.840.1.114404.1.1.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.3 |
| 8. | Extended Validation (“EV”) Code Signing Certificate* | EV Code Signing Certificate | 2.16.840.1.114404.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.4 |
| 9. | Organization Validation (“OV”) Web Server SSL Digital Certificate | OV Certificate | 2.16.840.1.114404.2.1.2<br>2.16.840.1.114404.1.1.2.3.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.4.3 |
| 10. | Domain Validation (“DV”) Web Server SSL Digital Certificate | DV Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.5.3 |
| 11. | Server All Purpose Certificate | Server All-Purpose Certificate, SAPCA Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.6.3 |
| 12. | Client All Purpose Certificate* | Client All-Purpose Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.7.3 |
| 13. | Timestamp Certificate* | Timestamp Certificate, Timestamp | 1.3.6.1.4.1.30360.3.3.3.3.4.8.3 |
| 14. | Document Signing Certificate* | Document Signing Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.9.3 |
| 15. | High Value Hierarchy Certification Authority Certificate* | HVCA Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.10.3 |

(*) As of June 1, 2010, this certificate type is not issued by Trustwave Holdings, inc. and consequently is only generally described herein.

# Trustwave Holdings, Inc.

Certification Practices and Certificate Policy Statement



### 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.

### Trustwave CA Corporate History

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

# 1 INTRODUCTION

This document is the ***Trustwave Certificate Policy and Certification Practices Statement*** ("Trustwave CP/CPS") which details the following information:

A. The legal and technical principles and practices that Trustwave employs in providing certification services,
B. The governing policies, practices, procedures, and infrastructure employed by The Trustwave Certification Authority ("CA") for its operations and business continuity,
C. The governing policies, practices and procedures employed in the creation, management, and termination of our root CA keys,
D. The governing policies, practices and procedures that apply to all End-Entity Digital Certificates ("Certificate") issued by our CA,
E. The physical, environmental, and logical security controls employed by Trustwave to protect our root CA certificates and keys, and
F. 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 to be employed throughout the lifetime of the Certificate. The Certificate lifecycle includes public and private key generation, the vetting of the information contained within the Certificate by the Trustwave CA, the CA signing of the Certificate, the implementation and use of the Digital Certificate, and finally, the termination of use of the Certificate. The governing policies, processes, and procedures associated with the issuance of digital certificates, as well as the interrelationship with the Trustwave Information Security Program by these governing policies, processes, and procedures of the different Certificate types are all detailed within this document.

Information Security services provided by Trustwave include:

- Certificate Generation, Update, Renewal, Re-key, and Distribution
- Certificate Revocation List (CRL) Generation and Distribution and Online Certificate Status Response Services
- Directory Management of Certificate Related Items
- Privilege and Authorization Management
- System Management Functions (e.g., security audit, configuration management, archive, etc.)

The security of these services is ensured by defining requirements on Trustwave CA activities, including the following:

- Subscriber identification and authorization verification
- Control of computer and cryptographic systems
- Operation of computer and cryptographic systems
- Usage of keys and certificates by Subscribers and relying parties
- Definition of rules to limit liability and to provide a high degree of certainty that the stipulations of this policy are being met

This CP/CPS focuses on the overall CA operations and the policies and procedures that govern the lifetime of the Trustwave Certification Authorities' "Private Keys" while also focusing on the policies and procedures encompassing the lifetime of all "End-Entity" Certificates.

This CP/CPS, along with all other documentation located at https://ssl.Trustwave.com/CA/, including relying party and subscriber agreements as well as the "Terms of Use" constitutes the obligations, representations, warranties, policies, and procedures that apply to any Digital Certificate issued by Trustwave.

The Trustwave Holdings, Inc. Certification Authority conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines shall take precedence over this document.

## 1.1 Overview

Trustwave operates and maintains three distinct Root Certification Authorities (hereinafter, collectively known as "Root CA", or "Trustwave Root CA") identified by the following names:

A. Secure Global Certification Authority ("SGCA")
B. XRamp Global Certification Authority ("XGCA")
C. SecureTrust Certification Authority ("STCA")

In addition, Trustwave maintains subordinate CAs (including the Trustwave Timestamp Authority, and hereinafter known as "Trustwave Subordinate CA(s)") that are subordinate to the Root CA. The entire hierarchy is depicted in the diagram below. This CP/CPS governs the operation and maintenance of, and is applicable to, the above-listed Root Certification Authorities as well as each of the subordinate CAs described below.

These certification authorities are collectively known as the ***"Trustwave Public Key Infrastructure Hierarchy"*** ("TPH").

1. Trustwave S/MIME Certification Authority ("SMCA"). This CA issues Certificates for S/MIME (secure e-mail) use.
2. Trustwave Code signing Certification Authority ("CSCA"). This CA issues Certificates for code signing use.
3. Trustwave Special Use Certification Authority ("SUCA"). This CA is reserved for Trustwave use only, issuing certificates for use within the Trustwave Certification Authority infrastructure itself.
4. Trustwave Independent Organization Certification Authority ("ORGCA"). This CA issues Certificates for an independent organization's certification authority use.
5. Trustwave Client Authentication Certification authority ("CLACA"). This CA issues "My Identity" client and server Certificates to be used for authentication purposes within a Virtual Private Network ("VPN").

6. Trustwave Internal SSL Certification Authority ("ISCA"). This CA issues certificates for server (e.g. WWW server) implementations to be used solely inside of an independent organization.
7. Trustwave Extended Validation Certification Authority ("EVCA"). This CA issues EV Certificates for server (e.g. WWW server) implementations. As of June 1, 2010, This CA does not, and has not, issued end entity certificates.
8. Trustwave Organization Validation Certification Authority ("OVCA"). This CA issues OV Certificates for server (e.g. WWW server) implementations.
9. Trustwave Domain Validation Certification Authority ("DVCA"). This CA issues DV Certificates for server (e.g. WWW server) implementations
10. Trustwave Server All Purpose Certification authority ("SAPCA"). This CA issues server Certificates that can be used for more than one purpose. (e.g. Server and client authentication in the same certificate).
11. Trustwave Client All Purpose Certification Authority ("CAPCA"). This CA issues client Certificates that can be used for more than one purpose (e.g. client authentication, and S/MIME capability in the same certificate). As of June 1, 2010, This CA does not, and has not, issued end entity certificates.
12. Trustwave Timestamp Authority ("TSA"). This capability responds only to time stamping requests. Trustwave
13. Document Signing Certification Authority ("DOCCA"). This CA issues certificates that are valid for document signing. As of June 1, 2010, This CA does not, and has not, issued end entity certificates.
14. Trustwave High Value Hierarchy Certification Authority ("HVHCA"). As of June 1, 2010, This CA does not, and has not, issued end entity certificates.

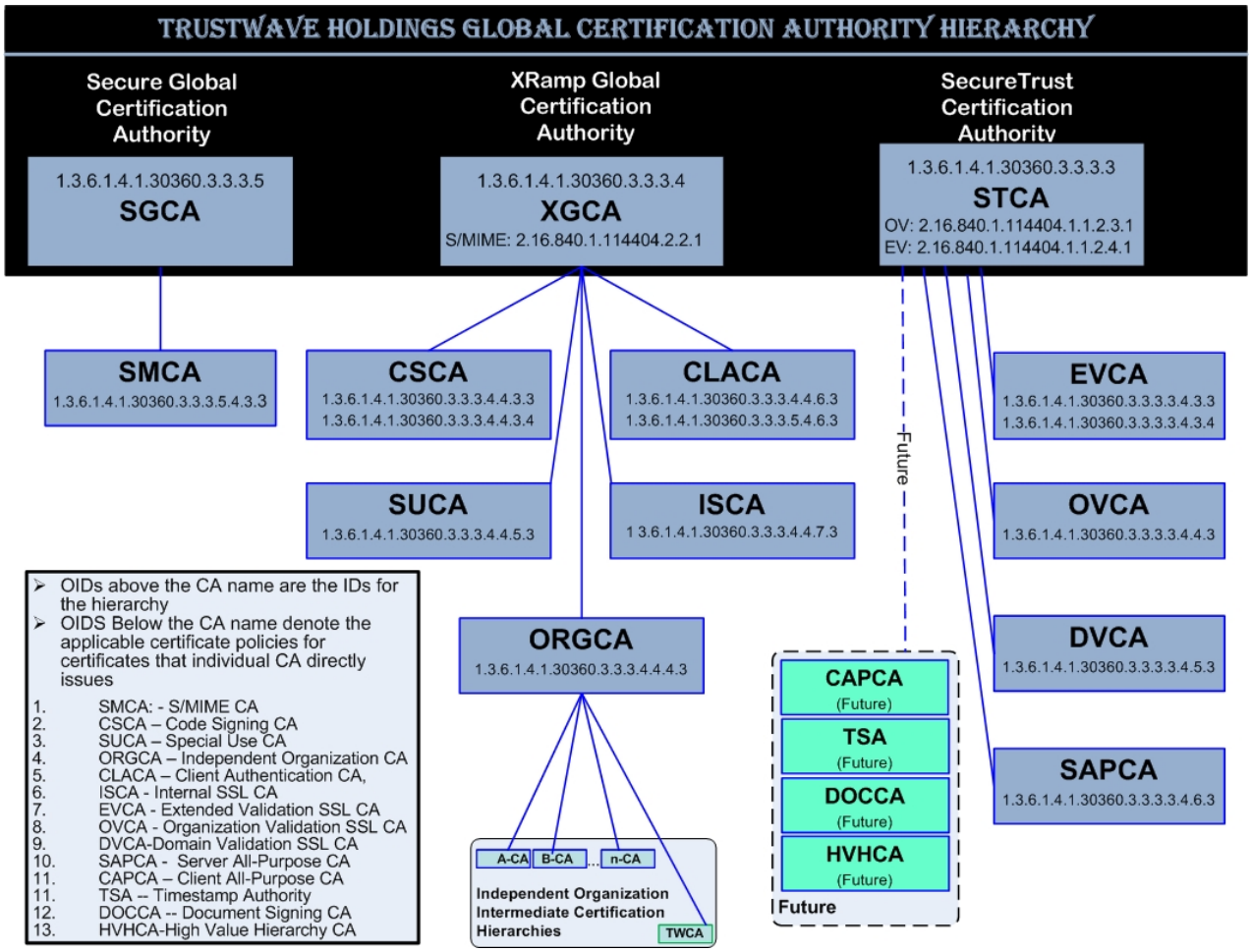


**Figure 1 - The Trustwave Holdings, Inc. Public Key Infrastructure**

Activities and governing policies of the TPH listed above and the Certificate Policies associated with the Certificates that each of these CAs issue are defined by this document. Certificate policies associated with certificate types that that have not been, or are not currently being, issued by Trustwave are not defined within this document. Certificate policies associated with these types of certificates will be defined in a future version of this CP/CPS prior to their issuance by Trustwave. The following Certificate Policies are NOT currently defined within this document, but may be defined at a later date:

| | *Certificate Type* | *Friendly Name* | *Certificate Policy ID* |
|---|---|---|---|
| 1. | Extended Validation ("EV") Code Signing Certificate* | EV Code Signing Certificate | 2.16.840.1.114404.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.4 |
| 2. | Client All Purpose Certificate* | Client All-Purpose Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.7.3 |
| 3. | Timestamp Certificate* | Timestamp Certificate, Timestamp | 1.3.6.1.4.1.30360.3.3.3.3.4.8.3 |

| | | | |
|---|---|---|---|
| 4. | Document Signing Certificate* | Document Signing Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.9.3 |
| 5. | High Value Hierarchy Certification Authority Certificate* | HVCA Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.10.3 |

Furthermore, the certificate policies and certification practices associated with the independent organization subordinate certification hierarchies beneath ORGCA and of the Certificates that these CAS issue are not defined within this document. However, the requirements for certification authority and certificate policy governance inclusion for all subordinate certification authorities underneath ORGCA are defined and contained herein.

All End-Entity Certificates issued by Trustwave shall contain a CP OID so that End-Entities and Relying Parties can identify the (i) type of Certificate, (ii) corresponding policies and procedures performed during the Certificate lifecycle including the vetting processes used prior to the issuance, (iii) intended purposes of the Certificate, and (iv) rights, responsibilities, and warranties for each party.

Applicants and Subscribers shall be responsible for:

- reviewing their certificate as issued by Trustwave to confirm the accuracy of the Subscriber information contained therein before first use,
- Using a trusted system for generating their key pair and to prevent any loss, disclosure, or unauthorized use of the private key,
- Keeping private keys confidential at all times,
- Keeping confidential, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to their private key and Trustwave PKI facilities,
- Making only true and accurate representations to the Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a certificate and for information contained within the certificate,
- In accordance with the Trustwave CP/CPS, exclusively using their Certificate for legal purposes and restricting its use to authorized purposes detailed by this document, and
- Immediately notifying Trustwave of a suspected or known key compromise in accordance with the procedures laid down in this Trustwave CP/CPS.

Relying parties shall be responsible for, and may justifiably rely upon a certificate only after:

- Ensuring that reliance on Certificates issued under this policy is restricted to appropriate uses as defined within this Trustwave CP/CPS,
- Ensuring that the Certificate remains valid and has not been revoked or suspended by accessing any and all relevant certificate status information, and
- Determining that such certificate provides adequate assurances for its intended use.

All of these Certificate Policies that further define these conditions are contained within this CP/CPS, the associated Relying Party Agreements, and Subscriber Agreements which can be found at https://ssl.trustwave.com/CA.

## 1.2 Document Name and Identification

This document is the ***Trustwave Certificate Policy and Certification Practices Statement*** ("Trustwave CP/CPS").

All certificates that Trustwave issues shall contain a CP OID corresponding to the applicable Certificate type. Because this CP/CPS is incorporated within all CPs, this CPS does not have a unique OID associated with it. This CP/CPS contains all relevant and current CPs.

Certificate Types indicated in **ORANGE**, within the table below, have not been, and are not currently being, issued by Trustwave. Correspondingly, certificate policies and the associated profiles of these certificate types are not defined within this document. However, operational policy and practice associated with the certification authorities, themselves, that would be capable of issuing these types of certificates is defined herein.

Trustwave issues the following Certificate types which can be identified by the Certificate Policy Object Identifier ("OID" or "CP OID") contained in the certificatePolicy extension within the End-Entity Certificate. This document identifies all Certificate Policy, as well as Certification Practice for the issuing CA, for any certificate type currently or previously issued by Trustwave. This document can be identified by the following certificate policy OIDs:

| | *Certificate Type* | *Friendly Name* | *Issuing Certification Authority* | *Certificate Policy OID* |
|---|---|---|---|---|
| 1. | Email S/MIME Digital Certificate | S/MIME Certificate, Secure E-Mail Certificate | XGCA[1]<br>SMCA | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.5.4.3.3 |
| 2. | Organization Validation ("OV") Code Signing Certificate | OV Code Signing Certificate | CSCA | 1.3.6.1.4.1.30360.3.3.3.4.4.3.4 |
| 3. | Special Use Certificate | SUCA Certificate | SUCA | 1.3.6.1.4.1.30360.3.3.3.4.4.5.3 |
| 4. | Independent Organization Certification Authority Certificate | ORGCA Certificate | ORGCA | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.4.4.4.3 |
| 5. | Client Authentication Certificate | Client Authentication Certificate, "My Identity" Certificate, VPN Certificate | CLACA | 1.3.6.1.4.1.30360.3.3.3.5.4.6.3<br>1.3.6.1.4.1.30360.3.3.3.4.4.6.3 |
| 6. | Internal SSL Certificate | ISSL Certificate | ISCA | 1.3.6.1.4.1.30360.3.3.3.4.4.7.3 |
| 7. | Extended Validation ("EV") Web Server SSL Digital Certificate | EV Certificate[†] | STCA<br>EVCA[2] | 2.16.840.1.114404.1.1.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.3 |

| | Certificate Type | Friendly Name | Issuing Certification Authority | Certificate Policy OID |
|---|---|---|---|---|
| 8. | **Extended Validation ("EV") Code Signing Certificate** | **EV Code Signing Certificate** | STCA<br>EVCA | **2.16.840.1.114404.2.4.1**<br>**1.3.6.1.4.1.30360.3.3.3.3.4.3.4** |
| 9. | Organization Validation ("OV") Web Server SSL Digital Certificate | OV Certificate | STCA<br><br>OVCA | 2.16.840.1.114404.2.1.2<br>2.16.840.1.114404.1.1.2.3.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.4.3 |
| 10. | Domain Validation ("DV") Web Server SSL Digital Certificate | DV Certificate | DVCA | 1.3.6.1.4.1.30360.3.3.3.3.4.5.3 |
| 11. | Server All Purpose Certificate | Server All-Purpose Certificate | SAPCA | 1.3.6.1.4.1.30360.3.3.3.3.4.6.3 |
| 12. | **Client All Purpose Certificate** | **Client All-Purpose Certificate** | CAPCA | **1.3.6.1.4.1.30360.3.3.3.3.4.7.3** |
| 13. | **Timestamp Certificate** | **Timestamp Certificate, Timestamp** | TSA | **1.3.6.1.4.1.30360.3.3.3.3.4.8.3** |
| 14. | **Document Signing Certificate** | **Document Signing Certificate** | DOCCA | **1.3.6.1.4.1.30360.3.3.3.3.4.9.3** |
| 15. | **High Value Hierarchy Certification Authority Certificate** | **HVCA Certificate** | HVHCA | **1.3.6.1.4.1.30360.3.3.3.3.4.10.3** |

(†)EV Certificates with a Validity Period starting on or after May 7, 2008 will follow this CP/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.

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

The only Certification Authority specifically governed by this document is the Trustwave CA. 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 components of the CP/CPS that govern the registration operations of their CA. All CAs that are listed in section 1.1 shall implement all requirements as listed within this statement.

### 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 CP/CPS. Third party RA's shall contractually agree to the terms of this CP/CPS, the relevant CPs, and the terms of their enterprise services agreement with Trustwave. RA's may, in their discretion, prescribe more restrictive practices. Furthermore, Trustwave shall perform a review and/or audit of all third party Registration Authority activities on a yearly basis.

Trustwave shall not enter into agreements with a third party to act as a Registration Authority with EV (EV SSL, or EV code signing) or OV code signing certificate issuance.

Common reasons that Trustwave contracts with a third party to be an RA includes servicing foreign markets, or servicing registration activity for "closed loop" institutions such as a large corporation, to perform identification and authentication of Applicants for Certificates. 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 CPs due to their knowledge of the local laws, business customs, and language.

### 1.3.3 Subscribers

Trustwave issues Certificates to *Individual, Private Organization, Government Entity, Business Entity and Non-Commercial End Entity Applicants* that satisfy the requirements contained within this document.

Subscribers are the End Entities that hold Certificates issued by Trustwave. A Subscriber can be an Individual, Private Organization, Government Entity, Business Entity, or Non-Commercial Entity, or any other type of legal entity. A Subscriber may also be Trustwave Holdings itself in the form of Certificates issued to subordinate CAs. Certificates issued to Trustwave employees, contractors, or devices shall assume the same obligations and requirements as any other End-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, Private Organization, Government Entity, Business Entity or Non-Commercial 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.

### 1.3.5 Other Participants

The three main participants in the Trustwave PKI are the Trustwave CA, Subscribers, and Relying Parties. However, a device can also have a Certificate associated with it that is not connected to a specific End Entity. 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

All certificates issued within the Trustwave Public Key Infrastructure Hierarchy shall have “key usage extensions” and may have "enhanced key usage” extensions, as defined within IETF RFC 5280 that defines acceptable usage of, and provide a basis for reliance upon, the private key corresponding to the Public Key that is contained within the Certificate.

**Non-repudiation**

IETF RFC 5280 defines the nonRepudiation assertion within the extended key usage extension as follows:

> *The nonRepudiation bit is asserted when the subject public key is used to verify digital signatures, other than signatures on certificates (bit 5) and CRLs (bit 6), used to provide a non-repudiation service that protects against the signing entity falsely denying some action. In the case of later conflict, a reliable third party may determine the authenticity of the signed data. (Note that recent editions of X.509 have renamed the nonRepudiation bit to contentCommitment.)*

**Trustwave does not and shall not assert the non-repudiation bit within any Certificate.**

**Trustwave shall not warrant any actions or activities by Subscribers based upon the Certificate and private key usage that has not been specifically indicated within the key usage and/or enhanced key usage extensions in conjunction with their definition as defined within this document.**

### 1.4.1 Appropriate Certificate Uses

As stated in Section 1.1, Trustwave issues many different types of Certificates, which are all intended for different purposes. The following table lists all certificate types that are issued, and have been issued, by Trustwave. The general description for each type’s permissible use is given within the following table:

| *Friendly Name* | *Certificate Policy ID* | *keyUsages* |
|---|---|---|
| 1. All Trustwave Subordinate CAs within the TPH | All. | • KU: **Digital Signature, Certificate Signing, CRL Signing**<br>• EKU: None |
| | The certificate defining any Trustwave CA, along with its associated private key, shall be used only to: 1) issue digital certificates to subscribers and subordinate CAs, and 2) sign certificate revocation lists that are applicable to its issued certificate population. | |
| 2. S/MIME Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.5.4.3.3 | • KU; **Digital Signature, Key Encipherment**<br>• EKU: Secure Email |
| | The Trustwave S/MIME Certificate that is issued to subscribers, along with its associated private key, shall be used only to enable secure e-mail communication. | |
| 3. OV Code Signing Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.3.4 | • KU; **Digital Signature**<br>• EKU: **Code Signing** |

| Friendly Name | Certificate Policy ID | keyUsages |
|---|---|---|
| | The Trustwave OV code signing Certificate as issued to subscribers, along with its associated private key, shall be used only to digitally sign application code. | |
| 4. SUCA Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.5.3 | • KU: Any<br>• EKU: Any |
| | Certificates issued by the Trustwave Special Use CA are used internally within the TPH to enable CA operations. **This CA issues one certificate to the Trustwave Certification Practice Board, and, along with its private key, is held by the Trustwave Holdings legal department, which may only be used to digitally sign this CP/CPS and other publicly available Trustwave CA documentation.** No public reliance on any certificate issued by this CA is warranted by Trustwave, except for this single certificate used to sign Trustwave CA documentation. If this certificate is in use, it shall be found at: https://ssl.trustwave.com/CA and shall only be relied upon for verifying the authenticity of Trustwave CA documentation. | |
| 5. ORGCA Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.4.4.4.3 | • KU: **Certificate Signing, CRL Signing**<br>• EKU: None |
| | The Trustwave Independent Organization CA of Trustwave, only issues certificates to subordinate CAs where the common name within the certificate identifies a non-Trustwave end entity for use within 'closed loop' infrastructures. For each of these subordinate certification authorities, Trustwave remains the authoritative issuing CA.<br>These certification authorities are primarily created to manage a large number of employees underneath a single business entity. | |
| 6. Client Authentication Certificate, "My Identity" Certificate, VPN Certificate | 1.3.6.1.4.1.30360.3.3.3.5.4.6.3<br>1.3.6.1.4.1.30360.3.3.3.4.4.6.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Client Authentication** |
| | These certificates shall be used only to enable client authentication within virtual private network construction. These certificates are issued to both Individuals (client authentication) and to the device (server authentication) to which these individuals shall connect for the purpose of a VPN authentication and tunnel construction | |
| 7. ISSL Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.7.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication** |
| | These certificates shall be only used internally within a non-Trustwave organization to enable TLS (SSL) communication. These certificates contain host names within the certificates subject that **are not resolvable** on the public Internet. | |
| 8. EV Certificate | 2.16.840.1.114404.1.1.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication** |
| | Trustwave EV certificates shall be used only to enable TLS (SSL) communication between a Web browser and a Web server. | |
| 9. OV Certificate | 2.16.840.1.114404.2.1.2<br>2.16.840.1.114404.1.1.2.3.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.4.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication,** Client Authentication |
| | Trustwave OV certificates shall be used only to enable TLS (SSL) communication between a Web browser and a Web server. | |

| Friendly Name | Certificate Policy ID | keyUsages |
|---|---|---|
| 10. DV Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.5.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication** |
| | Trustwave DV certificates shall be used only to enable TLS (SSL) communication between a Web browser and a Web server. | |
| 11. Server All-Purpose Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.6.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication, Client Authentication** |
| | Trustwave server all-purpose certificates shall be used to enable TLS (SSL) communication between a Web browser and a Web server, while simultaneously allowing that Web server to perform client authentication to another device. | |

### 1.4.2 Prohibited Certificate Uses

As a general rule, **other than certificates issued from DOCCA (currently inactive) and SUCA, no certificate issued from any other Trustwave CA shall possess or be recognized as possessing the capability of digitally signing any type of document (contract, legal letter, etc.).**

Certificates issued by Trustwave shall be used, and relied upon, only to the extent that the use is consistent with applicable law, including without limitation, applicable export or import laws. Furthermore, Trustwave shall not warrant any Relying Party's use of a Trustwave issued Certificate where the use or intended use by a Relying Party is not defined within this document.

Trustwave Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject. As such, a Trustwave Certificate is ***not*** intended to, nor does Trustwave, provide any assurances, or otherwise represent or warrant:

A. That the Subject named in the Certificate is actively engaged in doing business;
B. That the Subject named in the Certificate complies with applicable laws;
C. That the Subject named in the Certificate is trustworthy, honest, or reputable in its business dealings; or
D. That it is "safe" to do business with the Subject named in the Certificate.

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 4.5.1. 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
70 West Madison Street, Suite 1050
Chicago, Illinois 60602
USA

### 1.5.3 Persons 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 CPs. The members of the CPB, as well as their tenure, are determined by the Board of Directors of Trustwave. As of June 1, 2010, the following Individuals comprise the CPB:

A. General Counsel
B. Executive Director
C. Chief Technology Officer

### 1.5.4 CPS and CP Approval Procedures

All changes and revisions to this CPS and the related CPs 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

Accounting Practitioner: A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants (IFAC)..

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

Affiliate: A corporation, partnership, joint venture or other entity controlling, controlled by or under common control with another entity as determined by reference to a QIIS, QGIS, QTIS, Verified Legal Opinion, or Verified Accountant Letter.

Applicant: The Natural Person, Private Organization, Business Entity, or Government Entity that applies for (or seeks renewal of) a Certificate naming it as the Subject.

Applicant Representative: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant: (i) who signs and submits, or approves a Certificate Request on behalf of the Applicant, and/or (ii) who signs and submits a Subscriber Agreement on behalf of the Applicant, and/or (iii) who acknowledges and agrees to the Certificate Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the Trustwave CA.

Application Software Vendor: A developer of Internet browser software or other relying-party application software that displays or uses certificates and distributes Root CA certificates.

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

Business Entity: Any entity that is neither a Private Organization nor a Government Entity as defined herein. Examples include general partnerships, unincorporated associations, and sole proprietorships.

Certificate: A public key certificate.

Certificate Approver: 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 EV Certificate Requests submitted by other Certificate Requesters.

Certification Authority: An organization that is responsible for the creation, issuance, revocation, and management of Certificates. Where the CA is also the Root CA, references to the CA will be synonymous with Root CA.

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.

Certification Practice Statement (CPS): One of several documents providing the framework under which certificates are created, issued, managed and used.

Certificate Revocation List (CRL): A regularly updated time-stamped list of revoked or invalid EV Certificates that is created and digitally signed by the Trustwave CA that issued the Certificates.

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

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

Contract Signer: 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.

Control: "Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.

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

Demand Deposit Account: A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account.

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.

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.

End-Entity (EE): A person, computer system, or a communications device that is a subject or user of a Certificate. An End-Entity is a Subscriber, a Relying Party, or both.

Entity: A Certification Authority, Registration Authority, or End-Entity.

ETSI TS 102 042 v2.1.2: European Telecommunications Standards Institute, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

EV Authority: A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV Certificate Request, to take the Request actions described in these Guidelines.

EV Certificate: A certificate that contains information specified in these Guidelines and that has been validated in accordance with these Guidelines.

EV Certificate Beneficiaries: Persons to whom the Trustwave CA and its Root CA make specified EV Certificate Warranties.

EV Certificate Renewal: The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the Trustwave CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV Certificate.

EV Certificate Reissuance: The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the Trustwave CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a 'valid to' date that matches that of the current EV Certificate.

EV Certificate Request: A request from an Applicant to the Trustwave CA requesting that the Trustwave CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.

EV Certificate Warranties: In conjunction with the Trustwave CA issuing an EV Certificate, the Trustwave CA and its Root CA, during the period when the EV Certificate is Valid, promise that the Trustwave CA has followed the requirements of these Guidelines and the CA's EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate.

EV Data: All EV Certificate Requests and data related thereto (whether obtained from the Applicant or otherwise) in the CA's possession or control or to which CA has access.

EV OID: An identifying number, in the form of an "object identifier," that is included in the *certificatePolicies* field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) by pre-agreement with one or more Application Software Vendor, marks the certificate as being an EV Certificate.

EV Policies: Auditable EV Certificate practices, policies and procedures, such as a certification practice statement (CPS) and certificate policy (CP), that are developed, implemented, and enforced by the Trustwave CA and its Root CA.

EV Processes: The keys, software, processes, and procedures by which the Trustwave CA verifies EV Data, issues EV Certificates, maintains a Repository, and revokes EV Certificates.

Extended Validation Certificate: See EV Certificate.

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.

Government Agency: In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private Organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of Business Entities, the government agency

in the jurisdiction of operation that registers business entities. In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.

Government Entity: A government-operated legal entity, agency, department, ministry, or similar element of the government of a country, or political subdivision within such country (such as a state, province,

High Risk Applicants: Applicants likely to be at a high risk of being targeted for fraudulent attacks.

Incorporating Agency: In the case of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the Private Organization was established (e.g., the government agency that issued the Certificate of Incorporation). In the case of a Government Entity, the entity that enacted the law, regulation, or decree establishing the legal existence of the Government Entity.

Independent Confirmation From Applicant: A confirmation of a particular fact received by the Trustwave CA pursuant to the provisions of this CP/CPS or binding upon the Applicant.

Individual: A natural person.

International Organization: An organization founded by a constituent document, e.g., charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments.

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

Jurisdiction of Incorporation: In the case of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the case of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

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

Legal Existence: A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Legal Practitioner: A person who is either a lawyer or notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.

Maximum Validity Period: The maximum time period for which the issued EV Certificate is valid. Also, the maximum period after CA verification that certain Applicant information may be relied upon in issuing an EV Certificate pursuant to these Guidelines.

Object Identifier: A unique alphanumeric/numeric identifier registered under the International Standards Organization's applicable standard for a specific object or object class.

OCSP Responder: An online software application operated under the authority of the Trustwave CA and connected to its Repository for processing EV Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol: An online Certificate-checking protocol that enables relying-party application software to determine the status of an identified Certificate. See also OCSP Responder

Parent Company: A company that Controls a Subsidiary Company as determined by reference to a QIIS, QGIS, QTIS, Verified Legal Opinion, or Verified Accountant Letter.

Place of Business: The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted.

Principal Individual: An Individual of a Private Organization, Government Entity, or Business Entity that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or agent authorized by such entity or organization to conduct business related to the request, issuance, and use of Certificates.

Private Key: The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create Digital Signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency in its Jurisdiction of Incorporation.

Public Key: The key of a Key Pair that MAY be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify Digital Signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

Public Key Infrastructure: A set of hardware, software, people, procedures, rules, policies, and obligations used to facilitate the trustworthy creation, issuance, management, and use of Certificates and keys based on Public Key Cryptography.

Qualified Auditor: An independent public accounting firm that meets the auditing qualification requirements specified in Section 8.7.4 of these Guidelines.

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.

Registered Agent: An Individual or entity that is: (i) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (ii) listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (i) above.

Registered Office: The official address of a company, as recorded with the Incorporating Agency, to which official documents are sent and at which legal notices are received.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include, but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency (OCC) or Office of Thrift Supervision (OTS)

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.

Regulated Financial Institution: A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities having regulatory authority over such financial institution based on the governmental, national, state or provincial, or local laws under which such financial institution was organized and/or licensed.

Relying Party: Any person (Individual or entity) that relies on a Valid Certificate. An Application Software Vendor is not considered a Relying Party when software

distributed by such Vendor merely displays information relating to a Certificate. In this document, the terms “Certificate user” and “Relying Party” are used interchangeably.

Repository: An online database of EV Certificate status information, either in the form of a CRL or an OCSP response.

Risk Assessments: Activities defined within the Trustwave information security program that: (i) identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any EV Data or EV Processes; (ii) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the EV Data and EV Processes; and (iii) assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Trustwave CA has in place to control such risks.

Root CA: The top level Certification Authority that issues the self-signed Root Certificate under which the Trustwave CA issues Certificates.

Root CA Key Pair: The Private Key and its associated Public Key held by the Root CA.

Root Certificate: The self-signed certificate issued by the Root CA to identify itself and to facilitate signing of certificates identifying its Subordinate CAs.

Root Key Generation Script: A documented plan of procedures to be performed for the generation of the Root CA key pair.

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

Security Plan: Security procedures, measures, and products designed to achieve the objectives set forth in The Trustwave Information Security Program to reasonably manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of all Trustwave Certification Authority, Applicant, and Subscriber Data and Processes, as well as the complexity and scope of the activities of the CA

Signing Authority: One or more Certificate Approvers designated to act on behalf of the Applicant.

Sovereign State: A state, or country that administers its own government, and is not dependent upon, or subject to, another power.

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

Subject: The organization identified as the Subject in the s*ubject:organizationNam*e field of a Certificate, whose identity is unambiguously bound to a Public Key also specified in the Certificate. An Applicant becomes a Subject when the Certificate it requested is issued.

Subject Organization Information: A set of information contained in a Certificate that is specified in Section 3.1.1 of this document.

Subordinate CA: A Certification Authority whose certificates are signed by the Root CA, or another Subordinate CA. Certificates issued by a Subordinate CA will be valid

if the appropriate OID(s) for that certificate type is specified within the certificatePolicies extension of the end entity.

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.

Subscriber / Subscribing Organization: (EV) The organization identified as the Subject in the *subject:* organizationName field of a Certificate issued pursuant to this CP/CPS, and, as qualified by the Jurisdiction of Incorporation information in an EV Certificate.

Subscriber Agreement: An agreement between the Trustwave CA and the Subject named or to be named in an EV Certificate that specifies the rights and responsibilities of the parties.

Subsidiary Company: A company that is controlled by a Parent Company as determined by reference to a QIIS, QGIS, QTIS, Verified Legal Opinion, or Verified Accountant Letter.

Superior Government Entity: Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.

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.

Terms of Use: Those provisions regarding the safekeeping and acceptable uses of a Certificate in accordance with a CPS and CP that an Applicant Representative acknowledges and accepts on behalf of an Applicant when such Applicant is an Affiliate of the CA

Translator: An Individual or Business Entity that the Trustwave CA has reason to believe possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.

Valid: A Certificate that has not expired and has not been revoked

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.

Validation Specialists: Personnel performing validation duties specified in these Guidelines

Verified Accountant Letter: A document meeting the requirements specified in Section 3.6.2 of this document.

Verified Legal Opinion: A document meeting the requirements specified in Section 3.6.1 of this document.

WebTrust EV Program: The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities.

WebTrust Program for CAs: The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities, available at http://www.webtrust.org/certauth fin.htm.

WebTrust Seal of Assurance: An affirmation of compliance resulting from the WebTrust Program for CAs.

### 1.6.1 Abbreviations

| | |
|---|---|
| AICPA | American Institute of Certified Public Accountants |
| BIPM | International Bureau of Weights and Measures |
| BIS | (US Government) Bureau of Industry and Security |
| CA | Certification Authority |
| ccTLD | Country Code Top-Level Domain |
| CEO | Chief Executive Officer |
| CFO | Chief Financial Officer |
| CICA | Chartered Accountants of Canada |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| COO | Chief Operating Officer |
| CP | Certificate Policy |
| CPA | Chartered Professional Accountant |
| CPS | Certification Practices Statement |
| CRL | Certificate Revocation List |
| CSO | Chief Security Officer |
| DBA | Doing Business As (also known as "Trading As") |
| EV | Extended Validation |
| FIPS | (US Government) Federal Information Processing Standard |
| FQDN | Fully Qualified Domain Name |
| gTLD | Generic Top-Level Domain |
| HSM | Hardware Security Module |
| IANA | Internet Assigned Numbers Authority |
| ICANN | Internet Corporation for Assigned Names and Numbers |
| IEC | International Electro-technical Commission |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |

| | |
|---|---|
| ITU | International Telecommunications Union |
| LLC | Limited Liability Company |
| NGO | Non-Governmental Organization |
| NIST | National Institute of Standards and Technology |
| NTP | Network Time Protocol |
| OCC | (US Government) Office of the Comptroller of the Currency |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OTS | (US Government) Office of Thrift Supervision |
| PIN | Personal Identification Number |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure - X.509 (IETF Working Group) |
| QGIS | Qualified Government Information Source |
| QTIS | Qualified Government Tax Information Source |
| QIIS | Qualified Independent Information Source |
| RA | Registration Authority |
| RFC | Request for Comments |
| RSA | Rivest-Shamir-Adelman Encryption Algorithm |
| SEC | (US Government) Securities and Exchange Commission |
| S/MIME | Secure MIME (Multipurpose Internet Mail Extensions) |
| SSL | Secure Sockets Layer |
| TLD | Top-Level Domain |
| TLS | Transport Layer Security |
| TPH | Trustwave Public-Key Hierarchy |
| TW | Trustwave |
| UTC(k) | National realization of Coordinated Universal Time |

## 1.7 Conventions

The Trustwave Certificate Policy is based on, and complies with, the ISO/IEC X.509: *Information Technology - Open Systems Interconnection - The Directory: Public-Key and Attribute Certificate Frameworks* specification and IETF RFC 3647 *PKI Certificate Policy and Certification Practice Framework*. The IETF Framework is used worldwide to ensure interoperability and conformance to a recognized standard that defines a uniform certificate policy content and construction.

Terms not otherwise defined in this CP/CPS shall be as defined in applicable agreements, user manuals, certification practice statements, and certificate policies (CP) of 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.

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

Trustwave shall maintain three separate Repositories:

A. **Certificate Repository**. Trustwave shall make available the three root CA certificates at https://ssl.trustwavecom/CA. Digital Certificates that are issued to End-Entities are stored on non-public file systems and in internal databases and shall not be made publicly available.
B. **Document Repository**. This Certificate Policy and Certification Practice Statement, Legal documents, associated CPs, Subscriber Agreements, Relying Party Agreements, and other documents related to Trustwave's actions as a Certificate Services Provider shall be made publicly available on our web site at the following URL: https://ssl.trustwavecom/CA.
C. **Certificate Status Information Repository**. Certificate status information is available through 1) publicly published Certificate Revocation List ("CRL") available at https://ssl.trustwavecom/CA and/or 2) other online Certificate status protocols such as OCSP. Every Certificate issued by any CA within the TPH and governed by this CP/CPS will contain information within the Certificate that will identify the location where Certificate status information can be found. Trustwave shall issue CRLs for all Trustwave certificate types, including subordinate certification authorities, on a daily basis.

## 2.2 Publication of Certification Information

Trustwave shall maintain and publish all past and current versions of this CP/CPS, including all associated CPs, 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.

Sensitive internal documents associated with information security plans, security controls, trade secrets, and other operational plans are not made publicly available.

A. Trustwave shall not publish End-Entity certificates in any form of a public repository.
B. Trustwave shall publish certificate status information for all certificate types at its Certificate Status Information Repository located at https://ssl.trustwave.com/CA.

## 2.3 Time or Frequency of Publication

Updates to this CP/CPS and the associated CPs are approved and published as set forth in Section 9.12 herein. Subscriber Agreements and Relying Party Agreements are published as necessary. Certificate status information is published as specified within Section 4.9.8. 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 to authorized 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

The Trustwave CA issues Certificates to Natural Person, Private Organization, Government Entity, Business Entity and Non-Commercial Entity subjects that satisfy the requirements specified below:

## 3.1 Naming

All Certificates issued by Trustwave certification authorities shall comply with the ISO/ITU X.500 naming convention.

### 3.1.1 Types of Names

All Certificates will have the subject field (and any subject alternative name extensions, if present) of the Distinguished Name set as per the following:

| *Certificate Type* | *Types of Names* |
|---|---|
| A. EV Certificate, ORGCA Certificate | In addition to the fully authenticated FQDN of the server, the subject in the Certificate shall include the following authenticated attributes as required by CA/Browser Forum Guidelines:<br>1. Organization name (OID 2.5.4.10) containing Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by Trustwave as provided herein.<br>2. Domain name (OID 2.5.4.3) containing one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV Certificates.<br>3. Business category (OID 2.5.4.15) containing one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity".<br>4. Jurisdiction of Incorporation or Registration including:<br>i. Locality (OID 1.3.6.1.4.1.311.60.2.1.1)<br>ii. State or province (OID 1.3.6.1.4.1.311.60.2.1.2)<br>iii. Country (OID 1.3.6.1.4.1.311.60.2.1.3)<br>5. Physical Address of Place of Business including:<br>i. Locality (OID 1.3.6.1.4.1.311.60.2.1.1)<br>ii. State or province (OID 1.3.6.1.4.1.311.60.2.1.2)<br>iii. Country (OID 1.3.6.1.4.1.311.60.2.1.3)<br>6. Registration Number (OID 2.5.4.5)<br>For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration shall be entered into this field in any one of the common date formats.<br><br>For Government Entities that do not have a Registration Number or readily verifiable date of creation, the Trustwave CA shall enter appropriate language to indicate that the Subject is a Government Entity.<br><br>For Business Entities, the Registration Number that was received by the Business Entity upon government registration shall be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats. |

| Certificate Type | Types of Names |
|---|---|
| B. OV Certificate, Client Authentication Certificate (Server devices, Server All-Purpose Certificate | In addition to the fully authenticated FQDN of the server, the commonName component of the subject in these Certificates shall include the following authenticated attributes:<br>1. Organization name (OID 2.5.4.10) containing Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by Trustwave as provided herein.<br>2. Domain name (OID 2.5.4.3) containing one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).<br>3. Wildcard certificates are allowed. |
| C. DV Certificate | In addition to the fully authenticated FQDN of the server, the commonName component of the subject in these Certificates shall include the following authenticated attributes:<br>1. Domain name (OID 2.5.4.3) containing one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).<br>2. Wildcard certificates are not allowed for DV Certificates. |
| D. S/MIME Certificate | The commonName shall contain a generic string – "Trustwave SMIME user". The subject alternative name will be set to the authenticated Subscriber's e-mail address. |
| E. OV Code Signing Certificate | The commonName (CN) component of the subject name in OV Code Signing Certificates shall include the subject's full legal name. In addition, the commonName component of the subject in these Certificates shall include the following authenticated attributes:<br>1. Organization name (OID 2.5.4.10) containing Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by Trustwave as provided herein.<br>2. Domain name (OID 2.5.4.3) containing one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). |
| F. Client Authentication Certificate (client) | In addition to the authenticated name of the Individual or device, the common name component of the subject in client authentication Certificates shall include the following attributes<br>1. Organization name (OID 2.5.4.10)<br>2. Physical Address of Place of Business including:<br>• Locality (OID 1.3.6.1.4.1.311.60.2.1.1)<br>• State or province (OID 1.3.6.1.4.1.311.60.2.1.2)<br>• Country (OID 1.3.6.1.4.1.311.60.2.1.3) |

| Certificate Type | Types of Names |
|---|---|
| G. ISSL Certificate | The commonName (CN) component of the server's subject name in the Certificates shall be a **non-Internet resolvable** FQDN. In addition, the commonName component of the subject in these Certificates shall include the following authenticated attributes:<br>1. Organization name (OID 2.5.4.10) containing Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by Trustwave as provided herein.<br>Trustwave shall verify on a best effort on-going basis that the common name within all ISSL certificates remains non-resolvable on the public Internet. |

### 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:

| Certificate Type | Description of the Need for the Name to be Meaningful |
|---|---|
| A. EV Certificate<br>B. OV Certificate,<br>C. OV code signing certificate<br>D. DV certificate<br>E. Client Authentication Certificate<br>F. ORGCA certificate<br>G. ORGCA Certificate<br>H. Client Authentication Certificate<br>I. Server All-Purpose Certificate | Trustwave ensures via the practices and procedures defined within this document, and in 3.2.2, that the subject name uniquely identifies the name of the Subscriber. |
| J. S/MIME Certificate<br>K. ISSL Certificate | No stipulation. |

### 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.

No stipulation on anonymity or pseudonymity is made in the case of ISSL certificates.

### 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 Certificates shall be determined as set forth below:

| *Certificate Type* | *Uniqueness of Name Requirement* |
|---|---|
| A. EV Certificate<br>B. OV Certificate<br>C. DV certificate<br>D. OV Code Signing Certificate<br>E. ORGCA Certificate<br>F. Client Authentication Certificate<br>G. Server All-Purpose Certificate | The subject of all Certificates issued by Trustwave shall be unique. |
| H. S/MIME Certificate | The subject of all SMIME Certificates shall be generic in the form of: "Trustwave SMIME user". The subject alternative name of all S/MIME Certificates shall be unique. |
| I. ISSL Certificate | No stipulation. |

### 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 and revoke the Certificate due to potential trademark infringement.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

All End-Entity applicants for all certificate types 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

*3.2.2.1 EV and ORGCA Certificates*

Trustwave will verify Applicant's legal existence, physical existence, operational existence, and domain control as shown below.

A. **Legal Existence**

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 that Applicant is listed in a current version of a QIIS.

If neither of the above conditions is 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.

### *3.2.2.2 OV Certificate, Server All Purpose Certificate, ISSL Certificate, Client Authentication Certificate (VPN devices)*

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:

1. 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.
2. Third-party statements showing the use of the organizational name such as: Bank Statements and Merchant Account Statements.
3. 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:

1. 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.
2. Any other means by which it can be reasonably established that Subscriber has control over the domain name listed in the Certificate request.

The primary 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.

### *3.2.2.3 OV Code Signing Certificate*

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 one of the following documents to Trustwave that shows reasonable proof that the organization is operating under the organizational name that is listed in their Certificate request:

1. 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.
2. Third-party statements showing the use of the organizational name such as: Bank Statements and Merchant Account Statements.
3. If the organization is a sole-proprietorship or the Certificate is being issued to an Individual, then Trustwave will accept a copy of his or her driver's license, government issued identity card, or passport.

The above mentioned documents will 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. **Authorization Validation.** To confirm authorization for a code signing certificate, Trustwave will contact an appropriate Organizational contact via postal mail, facsimile, telephone, or other comparable means to verify that the organization has authorized the Certificate request and that the Individual submitting the Certificate Request is authorized to do so.

### 3.2.3 Authentication of Individual Identity -

#### *3.2.3.1 Client Authentication Certificate (Individuals)*

The applicable Sponsor will determine that an Applicant is an employee or contractor of the organization through correlation with Human Resources and contractor records prior to enrollment in the program. Furthermore, the applicable Sponsor shall ensure that all employees, contractors, vendors and any other Individual issued a certificate shall execute a confidentiality agreement wherein, he or she agrees to maintain all of the applicable Sponsor and Trustwave proprietary data, including without limitation all non-public information regarding the TPH, in strict confidence.

Acceptable means of correlation by the applicable Sponsor shall include, but is not limited to the following:

A. Trustwave or the applicable Sponsor shall receive one official identification document as issued by governmental authorities having the jurisdiction to issue such documents.
B. At least one document shall contain a picture of the current likeness of the Individual Applicant.
C. Any one of these documents must always be presented:
    1. Driver's license or identification card as issued by the state or locale of the Applicant's legal residence;
    2. U.S. Passport;
    3. Certified birth certificate issued by the city, county, or state of birth, in accordance with applicable law;
    4. Naturalization Certificate issued by a court of competent jurisdiction prior to October 1, 1991, or the U.S. Citizenship and Immigration Service (USCIS), formerly the Immigration and Naturalization Service (INS), since that date;
    5. Certificate of Citizenship issued by USCIS;
    6. Department of State Form FS-240 – Consular Report of Birth; or
    7. Department of State Form DS-1350 – Certification of Report of Birth.

8. For verification of non-US citizens, the applicant must present passport(s) issued by the country(ies) of citizenship.

D. Additionally, the employer must possess a current and valid 1099 form or W-4 form that matches the name associated with the preceding identity verification list.

*3.2.3.2 S/MIME Certificate*

S/MIME Certificates issued under this CP/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:

A. Trustwave receives a request for an S/MIME Certificate.
B. 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.
C. The Applicant shall click on the link which will take them to a webpage.
D. The Applicant then confirms their information and clicks a button asking for the Certificate to be issued.
E. 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 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

| *Certificate Type* | *Description* |
|---|---|
| A. EV Certificate, ORGCA Certificate | **Verification of Contract Signer / Certificate Approver**<br>For both the Contract Signer and the Certificate Approver, Trustwave shall verify each of the following:<br>A. 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 the Applicant;<br>B. 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");<br>C. 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:<br>1. Submit, and, if applicable, authorize a Certificate Requester to submit, the Certificate Request on behalf |

| Certificate Type | Description |
|---|---|
| | of Applicant; and<br>2. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from Applicant by the Trustwave CA for issuance of the Certificate; and<br>3. Approve Certificate Requests submitted by a Certificate Requester.<br><br>Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include:<br><br>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.<br>ii. Agency. Trustwave may verify agency of the Contract Signer and the Certificate Approver by:<br>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<br>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<br>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.<br><br>Acceptable methods of verification of the Signing Authority of the Contract Signer, and the authority of the Certificate Approver, as applicable, include:<br><br>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<br>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<br>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 |

| Certificate Type | Description |
|---|---|
| | 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<br>iv. Independent Confirmation from Applicant The Signing Authority of the Contract Signer, and/or been the authority of the Certificate Approver, may be verified by obtaining an Independent Confirmation from Applicant; or<br>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.<br><br>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:<br>i. the name and title of the Contract Signer and that he/she is an employee or agent of Applicant, and<br>ii. the Signing Authority of such Contract Signer in accordance with one of the procedures set forth above,<br>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. |
| B. OV Certificate, | See 3.2.2 |

| Certificate Type | Description |
|---|---|
| OV Code Signing Certificate Client Authentication Certificate, Server All Purpose Certificate, ISSL Certificate | |

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 CP/CPS, and for all Certificates issued within the TPH, Renewal Certificate Applications are subject to the same authentication steps outlined in this CP/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.

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.

Trustwave reserves the right to unilaterally revoke any certificate issued within the TPH without cause.

### 3.4.3 Procedure For Revocation Request

See section 4.9.3

## 3.5 Other Verification Requirements

### 3.5.1 High Risk Status

*3.5.1.1 Verification Requirements.*

Trustwave takes reasonable measures to identify high risk Applicants likely to be targeted for fraudulent attacks ("High Risk Applicants"). Trustwave conducts additional verification and takes reasonable precautions necessary to ensure that such Applicants are properly verified in accordance with the CA/Browser Forum Guidelines.

*3.5.1.2 Acceptable Methods of Verification.*

Trustwave may identify High Risk Applicants by checking appropriate lists of organization names that are most commonly targeted in phishing and other fraudulent schemes, and automatically flagging EV Certificate Requests from Applicants named on these listed for further scrutiny before issuance. Examples of such lists include: Anti-Phishing Work Group list of phishing targets and internal Trustwave databases that include previously revoked EV Certificates and previously rejected EV Certificate Requests due to suspected phishing or other fraudulent usage. This information is then used to flag suspicious new EV Certificate Requests. If an Applicant is flagged as a High Risk Applicant, Trustwave performs reasonably appropriate additional authentication and verification to be certain beyond reasonable doubt that Applicant and the target in question are the same organization.

### 3.5.2 Denied Lists and Other Legal Black Lists

*3.5.2.1 Verification Requirements*

Trustwave must verify whether the Applicant, the Contract Signer, the Certificate Approver, Applicant's Jurisdiction of Incorporation, Registration, or Place of Business:

A. Is identified on any government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the United States; or
B. Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the law of the United States prohibits doing business.

Trustwave does not issue any EV Certificates to Applicants if either Applicant, the Contract Signer, or Certificate Approver, or if Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

*3.5.2.2 Acceptable Methods of Verification*

Trustwave takes reasonable steps to verify with the following lists and regulations:

A. BIS Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp
B. BIS Denied Entities List - http://www.bis.doc.gov/entities/default.htm
C. U.S. Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/offices/enforcement/ofac/sdn/t11sdn.pdf
D. U.S. Government export regulations

## 3.6 Verification of Certain Information Sources

### 3.6.1 Verified Legal Opinion

*3.6.1.1 Verification Requirements*

Before relying on any legal opinion submitted to Trustwave, Trustwave will verify that such legal opinion meets the following requirements ("Verified Legal Opinion"):

A. Status of Author

Trustwave will verify that the legal opinion is authored by an independent legal practitioner retained by and representing Applicant (or an in-house legal practitioner employed by Applicant) (Legal Practitioner) who is either:

1. A lawyer (or solicitor, barrister, advocate, or equivalent) 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; or
2. A notary that is a member of the International Union of Latin Notaries, and is licensed to practice in the country of Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary).

B. Basis of Opinion

Trustwave will verify that the Legal Practitioner is acting on behalf of Applicant and that the conclusions of the Verified Legal Opinion is based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise.

C. Authenticity

Trustwave will confirm the authenticity of the Verified Legal Opinion.

*3.6.1.2 Acceptable Methods of Verification*

Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:

A. Status of Author

Trustwave will verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering

or licensing such Legal Practitioner(s) in the applicable jurisdiction.

B. Basis of Opinion

The text of the legal opinion must make it clear that the Legal Practitioner is acting on behalf of Applicant and that the conclusions of the legal opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion may also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous.

C. Authenticity

To confirm the authenticity of the legal opinion, Trustwave will make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, Trustwave may use the number listed for the Legal Practitioner in records provided by the applicable phone company, a QGIS, or a QIIS. In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by Trustwave in Section 22(a)(2)(A), no further verification of authenticity is required.

### 3.6.2 Verified Accountant Letter

*3.6.2.1 Verification Requirements*

Before relying on any accountant letter submitted, Trustwave will verify that such accountant letter meets the following requirements ("Verified Accountant Letter"):

A. Status of Author

Trustwave shall verify that the accountant letter is authored by an independent Accounting Practitioner retained by and representing the Applicant (or an in-house professional accountant employed by the Applicant) who is a certified public accountant, chartered accountant, or has an equivalent license within the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or the jurisdiction where the Applicant maintains an office or physical facility. Verification of license MUST be through that jurisdiction's member of the International Federation of Accountants (IFAC) or through the regulatory organization in that jurisdiction appropriate to contact when verifying an accountant's license to practice in that jurisdiction;

B. Basis of Opinion

Trustwave will verify that the Accounting Practitioner is acting on behalf of Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise.

C. Authenticity

Trustwave will confirm the authenticity of the Verified Accountant Letter.

*3.6.2.2 Acceptable Methods of Verification*

Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are:

A. Status of Author

Trustwave will verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.

B. Basis of Opinion

The text of the accountant letter must make clear that the Accounting Practitioner is acting on behalf of Applicant and that the information in the accountant letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The accountant letter may also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the accountant letter prove to be erroneous.

C. Authenticity

To confirm the authenticity of the accountant's opinion, Trustwave will make a telephone call or send a copy of the accountant letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, Trustwave may use the number listed for the Accountant in records provided by the applicable phone company, a QGIS, or a QIIS. In circumstances where the opinion is digitally signed, in a manner that confirms the

authenticity of the document and the identity of the signer, as verified by Trustwave, no further verification of authenticity is required

### 3.6.3 Face-to-face Validation

*3.6.3.1 Verification Requirements*

Before relying on any face-to-face vetting documents submitted, Trustwave must verify that the Third-Party Validator meets the following requirements:

A. Qualification of Third-Party Validator

Trustwave must independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the Individual's residency;

B. Document chain of custody

Trustwave must verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the Individual being validated

C. Verification of Attestation

If the Third-Party Validator is not a Latin Notary, then Trustwave must confirm the authenticity of the attestation and vetting documents.

*3.6.3.2 Acceptable Methods of Verification*

Acceptable methods of establishing the foregoing requirements for vetting documents are:

A. Qualification of Third-Party Validator

Trustwave must verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction.

B. Document Chain of Custody

The Third-Party Validator must submit a statement to the Trustwave which attests that they obtained the Vetting Documents submitted to Trustwave for the Individual during a face-to-face meeting with the Individual.

C. Verification of Attestation

If the Third-Party Validator is not a Latin Notary, then Trustwave must confirm the authenticity of the vetting documents received from the Third-Party Validator. Trustwave must make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. Trustwave may rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by Trustwave, no further verification of authenticity is

required.

### 3.6.4 Independent Confirmation from Applicant

An "Independent Confirmation from Applicant" is a confirmation of a particular fact (e.g., knowledge of its exclusive control of a domain name, confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the EV Authority of a Certificate Approver, etc.) that is:

A. Received by Trustwave from a person employed by Applicant (other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact ("Confirming Person"), and who represents that he/she has confirmed such fact;
B. Received by Trustwave in a manner that authenticates and verifies the source of the confirmation; and
C. Binding on Applicant.

#### *3.6.4.1 Procedures for Independent Confirmation from Applicant*

An Independent Confirmation from Applicant may be obtained via the following procedure:

A. Confirmation Request.

Trustwave must initiate an appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue ("Confirmation Request") as follows:

1. Addressee. The Confirmation Request is directed to:

i. A position within Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, a Verified Accountant Letter, or by 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 this CP/CPS); or

ii. Applicant's Registered Agent or Registered Office in the Jurisdiction of Incorporation as listed in the official records of the Incorporating Agency, with instructions that it be forwarded to an appropriate Confirming Person; or

iii. A named Individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by 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 Guidelines).

2. Means of Communication. The Confirmation Request is directed to the Confirming Person in a manner reasonably likely to reach such

person. The following options are acceptable:

i. By paper mail addressed to the Confirming Person at:

a. The address of Applicant's Place of Business as verified by the Trustwave CA in accordance with this CP/CPS; or

b. The business address for such Confirming Person specified in a current Qualified Government Information Source (e.g., an SEC filing), a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or

c. The address of Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation; or

ii. By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current Qualified Government Information Source, a Qualified Government Tax Information Source, a Qualified Independent Information Source, a Verified Legal Opinion, or a Verified Accountant Letter; or

iii. By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of Applicant's Place of Business (verified in accordance with these Guidelines) and asking to speak to such person, and a person taking the call identifies himself as such person; or

iv. By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current Qualified Government Information Source, a Qualified Independent Information Source, a Qualified Government Tax Information Source, a Verified Legal Opinion, or a Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

B. Confirmation Response

Trustwave must receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response may be provided to Trustwave by telephone, by e-mail, or by paper mail, so long as Trustwave can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

C. The Trustwave CA MAY rely on a verified Confirming Person to confirm their own contact information: email address, telephone number, and facsimile number. The Trustwave CA MAY rely on this verified contact information for future correspondence with the

Confirming Person if:

1. The domain of the e-mail address is owned by the Applicant and is the Confirming Person's own e-mail address and not a group e-mail alias; or
2. The Confirming Person's telephone/fax number is verified by the Trustwave CA to be a telephone number that is part of the organization's telephone system, and is not the personal phone number for the person.

### 3.6.5 Qualified Independent Information Sources (QIIS)

A QIIS is 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:

A. Data it contains that will be relied upon has been independently verified by other independent information sources;
B. The database distinguishes between self-reported data and data reported by independent information sources;
C. The database provider identifies how frequently they update the information in their database;
D. Changes in the data that will be relied upon will be reflected in the database in no more than 12 months; and
E. The database provider uses authoritative sources independent of the subject, or multiple corroborated sources, to which the data pertains.

Databases in which Trustwave or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities (RAs) or subcontractors to whom Trustwave has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest do not qualify as a QIIS. Trustwave must check the accuracy of the database and ensure its data is acceptable.

### 3.6.6 Qualified Government Information Source (QGIS)

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 provided they are maintained by a Government Entity, the reporting of data is required by law and false or misleading reporting is punishable with criminal or civil penalties. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

### 3.6.7 Qualified Government Tax Information Source (QGTIS)

A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g. the I.R.S. in the United States). .

# 4 CERTIFICATE LIFECYCLE OPERATIONAL REQUIREMENTS

This CP/CPS defines operational policies and the requirements of our Certification Authority that pertain to all types of Certificates issued from any Trustwave CA.

## 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.

| *Certificate Type* | *Application Submission Criteria* |
|---|---|
| A. EV Certificate | 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 and of section 4.1.1.1 EV Certificate Applicant Requirements. |
| B. OV Certificate, ISSL Certificate, Server All-Purpose Certificate | 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:<br>1) A Verified Legal Opinion or Verified Accountant Letter which states that the Certificate requester has Certificate requesting authority;<br>2) 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;<br>3) 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<br>4) Trustwave and Applicant may mutually enter into a contract which states that the Certificate requester has requesting authority. |
| C. OV Code Signing Certificate | 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:<br>1) A Verified Legal Opinion or Verified Accountant Letter which states that the Certificate requester has Certificate requesting authority;<br>2) 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;<br>3) 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<br>4) Trustwave and Applicant may mutually enter into a contract which states that the Certificate requester has requesting authority. |
| D. S/MIME Certificate, DV Certificate | No stipulation. |

| Certificate Type | Application Submission Criteria |
|---|---|
| E. 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 |
| F. Client Authentication Certificate | The initial application for the client authentication Certificate shall be requested by employees of an organization such that they meet the requirements of section 3.2.5 Validation of Authority. |

*4.1.1.1 EV Certificate Applicant Requirements*

Trustwave MAY issue EV Certificates to Private Organization, Government Entity, Business Entity and Non-Commercial Entity subjects that satisfy the requirements specified below.

**A. Private Organization Subjects**

Trustwave MAY issue EV Certificates to Private Organizations that satisfy the following requirements:

1. The Private Organization MUST be a legally recognized entity whose existence was created by a filing with (or an act of) the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration (e.g., by issuance of a certificate of incorporation) or is an entity that is chartered by a state or federal regulatory agency;
2. The Private Organization MUST have designated with the Incorporating or Registration Agency either a Registered Agent, or a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration) or an equivalent facility;
3. The Private Organization MUST NOT be designated on the records of the Incorporating or Registration Agency by labels such as “inactive,” “invalid,” “not current,” or the equivalent;
4. The Private organization MUST have a verifiable physical existence and business presence;
5. The Private Organization’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business MUST NOT be in any country where Trustwave is prohibited from doing business or issuing a certificate by the laws of Trustwave’s jurisdiction; and
6. The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Trustwave’s jurisdiction.

**B. Government Entity Subjects**

Trustwave MAY issue EV Certificates to Government Entities that satisfy the following requirements:

1. The legal existence of the Government Entity MUST be established by the political subdivision in which such Government Entity operates;
2. The Government Entity MUST NOT be in any country where Trustwave is prohibited from doing business or issuing a certificate by the laws of Trustwave's jurisdiction; and
3. The Government Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Trustwave's jurisdiction.

**C. Business Entity Subjects**

Trustwave MAY issue EV Certificates to Business Entities who do not qualify under Section A but that do satisfy the following requirements:

1. The Business Entity MUST be a legally recognized entity whose formation included the filing of certain forms with the Registration Agency in its jurisdiction, the issuance or approval by such Registration Agency of a charter, certificate, or license, and whose existence can be verified with that Registration Agency;
2. The Business Entity MUST have a verifiable physical existence and business presence;
3. At least one Principal Individual associated with the Business Entity MUST be identified and validated;
4. The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;
5. Where the Business Entity represents itself under an assumed name, Trustwave MUST verify the Business Entity's use of the assumed name pursuant to the requirements herein;
6. The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be located or residing in any country where Trustwave is prohibited from doing business or issuing a certificate by the laws of Trustwave's jurisdiction; and
7. The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Trustwave's jurisdiction.

**D. Non-Commercial Entity Subjects**

Trustwave MAY issue EV Certificates to Non-Commercial Entities who do not qualify under Sections A, B or C, but satisfy the following requirements:

**1. International Organization Entities**

i. The Applicant is an International Organization Entity, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. Trustwave/Browser Forum may publish a listing of International Organizations that have been approved for EV eligibility; and

ii. The International Organization Entity MUST NOT be headquartered in any country where Trustwave is prohibited from doing business or issuing a certificate by the laws of Trustwave's jurisdiction; and

iii. The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of Trustwave's jurisdiction.

### 4.1.2 Enrollment Process and Responsibilities

For all certificate types, the applicant shall submit a PKCS #10 Certificate Signing Request ("CSR") for initial application processing.

| *Certificate Type* | *Enrollment Process and Responsibilities* |
|---|---|
| A. EV Certificate, ORGCA Certificate | Role Requirements. The following Applicant roles are required for the issuance of an EV, EV code signing, or subordinate CA Certificate.<br>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.<br>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.<br>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.<br>d.) Applicant Representative: Terms of Use applicable to the requested EV Certificate must be acknowledged and agreed to by an authorized Applicant Representative.<br><br>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.<br><br>Following completion of contract arrangements as per section 3.2.5, the applicant shall submit the PKCS #10 Certificate Signing Request ("CSR") for initial application processing. |
| B. OV Certificate, OV Code Signing Certificate, S/MIME Certificate, Client Authentication Certificate, Server All-Purpose Certificate, ISSL Certificate | Applicants for Certificates to be issued by Trustwave shall follow the registration procedures as defined by the Trustwave.<br>The primary steps for a Certificate registration are:<br>1. Valid identification documentation is provided and complete registration forms have been signed;<br>2. The CP/CPS and End-User Agreement have been accepted by the Subscriber; and<br>3. All documents and information provided by Applicant are approved by Trustwave. |

| | |
|---|---|
| C. DV Certificate | The primary steps for a Certificate registration are:<br>• Valid identification documentation is provided and complete registration forms have been signed;<br>• The CP/CPS and End-User Agreement have been accepted by the Subscriber; and<br>• All documents and information provided by Applicant are approved by Trustwave.<br><br>Trustwave shall enroll the applicant by either<br><br>1. Email Address White list<br>This validation method relies upon the Trustwave CA sending the unique provisioning token and certificate issuance URL to one or more recipients belonging to the following list of recipients:<br>a. root@domain<br>b. admin@domain<br>c. administrator@domain<br>d. webmaster@domain<br>e. hostmaster@domain<br>f. Any address listed in the contact fields of the domain's WHOIS record.<br>2. Domain Beacon<br>This validation method relies upon an Applicant placing specific content at a predefined location at the domain for which the request is being made. This page may be http rather than https since the Applicant may not currently possess a Certificate. . |

## 4.2 Certificate Application Processing

### 4.2.1 Performing Identification and Authentication Functions

| *Certificate Type* | *Identification and Authentication Functions* |
|---|---|
| A. EV Certificate, ORGCA Certificate | 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:<br><br>1. Verification of Applicant's existence and identity, including:<br>• Verify Applicant's legal existence and identity<br>• Verify Applicant's physical existence<br>• Verify Applicant's operational existence<br>2. Verify Applicant is a registered holder or has exclusive control of the domain name<br>3. Verify Applicant's authorization for requesting the Certificate including:<br>• Verify the name, title, and authority of the contract signer, Certificate Approver, and Certificate Requester.<br>• Verify that Contract Signer signed the Subscriber Agreement, and<br>• Verify that a Certificate Approver has signed or otherwise approved the Certificate request<br><br>**Maximum Validity Period for Validated Data**<br><br>The age of validated data used to support issuance of a Certificate (before revalidation is required) shall not exceed the following limits:<br><br>A. Legal existence and identity – 13 months;<br>B. Assumed name – 13 months;<br>C. Address of Place of Business – 13 months, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source |

| Certificate Type | Identification and Authentication Functions |
|---|---|
| | D. Telephone number for Place of Business – 13 months;<br>E. Bank account verification – 13 months;<br>F. Domain name – 13 months;<br>G. Identity and authority of Certificate Approver – 13 months, 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.<br><br>**Note on Reuse and Updating Information and Documentation**<br><br>a. Use of Documentation to Support Multiple Certificates<br>Trustwave may, at its own discretion, issue multiple Certificates listing the same Subject and based on a single Certificate Request, subject to the aging and updating requirement in (b) below.<br>b. Use of Pre-Existing Information or Documentation<br>(1) Each Certificate issued by Trustwave must be supported by a valid current Certificate Request and a Subscriber Agreement signed by the appropriate Applicant Representative on behalf of Applicant or Terms of Use acknowledged by the appropriate Applicant Representative.<br>(2) The age of information used by Trustwave to verify such an 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).<br>(3) In the case of outdated information, Trustwave shall repeat the verification processes required in this CP/CPS. |
| B. OV Certificate, ISSL Certificate, Server All Purpose certificate, | 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. |
| C. OV Code Signing Certificate | 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. |
| D. S/MIME Certificate | S/MIME Certificates issued under this CP/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 |

| Certificate Type | Identification and Authentication Functions |
|---|---|
| | following the request/response mechanism in 3.2.3. |
| E. Client Authentication Certificate (Individuals) | The applicable Sponsor shall implement a high-level view of the procedures carried out in the determination of the legal name of the employee to be included within the Certificate. The applicable Sponsor will determine the validity of the employee or contractor legal name through correlation with Human Resources and contractor records prior to the enrollment in the program.<br><br>Acceptable means of correlation by the applicable Sponsor may include the following:<br><br>• A designated representative from the Applicant's company, or a Trustwave employee, shall be responsible for collecting the two components of identity evidence (see 3.2.2) associated with the Applicant.<br>• The designated representative from the Applicant's company, or a Trustwave employee, shall verify that the photograph from the representative documentation collected in 3.2.2 is a reasonable likeness of the Applicant.<br>• The designated representative from the Applicant's company, or a Trustwave employee, shall provide the Applicant via face-to-face contact, via telephone, or via email with a single use time-limited password.<br>• Trustwave shall attribute the password provided to the Applicant to a profile stored on Trustwave enrollment servers.<br>• The Applicant shall connect to Trustwave's secure enrollment servers over TLS from their client computer and initiate key generation routines. Upon completion of the Applicant's key generation routines, the Applicant must provide a valid e-mail address for notification upon completion of the Certificate generation by Trustwave. Furthermore, the Applicant will be provided with a single use pass code, necessary for collection of the client authentication Certificate upon issuance by Trustwave.<br><br>Using the pass code provided within the browser in the previous step, the Applicant shall connect to the Trustwave enrollment servers to receive the final Certificate. |
| F. DV certificate | See 4 .1 .2 |

#### 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:

A. EV Certificates, Organizational CA Certificates – 10 business days
B. All other certificate types - two business days

### 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 or ORGCA 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 CP/CPS, Trustwave may include a Latin character organization name in an EV or an ORGCA 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 Trustwave 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 Trustwave 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 Certificates, shall

A. Possess at least a rudimentary knowledge of public key cryptography and Certificates;
B. Have completed all necessary enrollment forms and have executed payment for all accounts due;

C. Read and agree to this CP/CPS, any and all relevant CPs, and any and all Subscriber Agreements;
D. Protect their private key from unauthorized access and Compromise;
E. Not share their private key and or passwords protecting their private key;
F. Notify Trustwave of any change to the information contained within the Certificate;
G. Comply with all laws and regulations applicable to the export, import, and use of Certificates issued by Trustwave; and.
H. Except as otherwise set forth herein, in no event, use a Certificate issue by Trustwave for the purpose of signing a document with the intent to authenticate and create a legally binding signature.

Certificates issued by Trustwave, and their associated private keys, shall only be used for the following scenarios:

| *Certificate Type* | *Private key and certificate usage* |
|---|---|
| EV Certificate, OV SSL, Server All Purpose Certificate, ISSL Certificate, DV Certificate | These Certificates shall only be used to provide for the Web server's TLS/SSL endpoint. These Certificates shall serve only to authenticate the Web server to a client. |
| S/MIME Certificate | These Certificates shall only be used to facilitate an S/MIME transaction between two e-mail addresses |
| OV Code Signing Certificate | These Certificates shall only be used to sign object or component code. |
| Client Authentication Certificate | These Certificates shall only be used to provide for client and server authentication for VPN tunnel endpoints. |

### 4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall:

A. possess at least a rudimentary knowledge of public key cryptography and Certificates and their associated risks;
B. read and agree to this CP/CPS, any and all relevant CPs, and any and all Relying Party Agreements;
C. 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;
D. comply with all laws and regulations applicable to the export, import, use and reliance on a Certificate issued by Trustwave

Relying parties shall not:

E. Rely on a digital signature within the TPH to be a legally binding signature, except as otherwise set forth herein.

## 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 Trustwave 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 CP/CPS, Re-key Certificate Applications are subject to the same authentication steps outlined in this CP/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 Trustwave 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 Trustwave CA to Other Entities

No stipulation.

## 4.9 Certificate Revocation and Suspension

#### 4.9.1 Revocation Guidelines and Capability

Trustwave maintains a continuous 24x7 ability to accept and respond to revocation requests and related inquiries.

Subscribers shall immediately notify Trustwave for the purpose of revocation if any of the following exist/occur:

A. The Subscriber determines that information contained within the certificate as issued by Trustwave is not accurate,

B. The Subscriber believes that their private key is or has been subject to a suspected or known key compromise,

C. The Subscriber believes that, any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to their private key or Trustwave PKI facilities has not remained confidential, or

D. The Subscriber has not made true and accurate representations to the Registration Authority and/or Issuing Authority as to the information required to determine eligibility for a Certificate and for information contained within the Certificate.

### 4.9.2 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:

A. The Subscriber requests revocation of its Certificate;
B. The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
C. 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;
D. Trustwave receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
E. 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;
F. Trustwave receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
G. A determination, in Trustwave's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the applicable CP;
H. Trustwave determines that any of the information appearing in the Certificate is not accurate;
I. Trustwave ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
J. Trustwave's Private Key for that Certificate has been compromised;
K. Such additional revocation events as Trustwave publishes; or
L. 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.
M. The Subscriber intentionally includes Suspect Code in its signed software.
N. Trustwave obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been used for purposes that have not been granted within the key usage and/or extended key usage extensions in the corresponding certificate.

### 4.9.3 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).

### 4.9.4 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.

### 4.9.5 Revocation Request Grace Period

See 4.9.3

### 4.9.6 Time within Which CA Must Process the Revocation Request

See 4.9.3

### 4.9.7 Revocation Checking Requirement for Relying Parties

Relying parties shall ensure that the Certificate remains valid and has not been revoked or suspended by accessing all relevant certificate status information.

### 4.9.8 CRL Issuance Frequency

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

### 4.9.9 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.

### 4.9.10 On-line Revocation/Status Checking Availability

No stipulation.

### 4.9.11 On-line Revocation Checking Requirements

No stipulation.

#### 4.9.12 Other Forms of Revocation Advertisements Available

No stipulation.

#### 4.9.13 Special Requirements Regarding Key Compromise

No stipulation.

#### 4.9.14 Circumstances for Suspension

No certification authority within the TPH shall suspend Certificates.

#### 4.9.15 Who Can Request Suspension

No stipulation.

#### 4.9.16 Procedure for Suspension Request

No stipulation.

#### 4.9.17 Limits on Suspension Period

No stipulation.

### 4.10 Certificate Status Services

#### 4.10.1 Operational Characteristics

CRL access for all Trustwave certificate types is located at the following URL:

**https://ssl.trustwave.com/CA**

#### 4.10.2 Service Availability

Trustwave shall provide a current CRL that is accessible by Relying Parties and Subscribers for checking the status of all Certificates in the certificate validation chain. The CRLs will be signed so that the authenticity and integrity of the CRLs can be verified.

#### 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 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:

A. power systems to ensure the operation of its servers and its network connections; and
B. 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:

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

Trusted Persons include, but are not limited to:

A. Customer service personnel;
B. Cryptographic business operations personnel;
C. Security personnel;
D. System administration personnel;
E. Designated engineering personnel; and
F. 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 as defined 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:

A. Issued access devices and granted access to the required facilities;
B. 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):

A. The Generation, Issuing, Backups, Or Destruction Of A Root CA Key Pair;
B. The Loading Of Root CA Keys On An HSM;
C. The Storage Of Or Access To Root CA Key Material; And
D. 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 CP/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:

A. Trustwave shall provide all employees and contractors interacting with the TPH in a role supporting extended validation 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.
B. Trustwave shall maintain all records associated with training of the employees and contractors within the TPH for seven years.
C. 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:

A. Social Security Number Verification;
B. Criminal Records Search;
C. Credit History Review;

D. Education Verification;
E. Employment History Verification; and
F. 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 CP/CPS, and all CA/Browser Forum Guidelines.

5.3.4 Retraining Frequency and Requirements

All Trustwave employees and contractors interacting with the TPH in a role supporting extended validation 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 CP/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 a role supporting extended validation are provided with the documentation necessary to perform the role to which they are assigned, including a copy of this CP/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:

A. Compliance with this CP/CPS and other obligations under Trustwave agreements with subscribers
B. 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:

A. CA key lifecycle management events, including:

1) Key generation, backup, storage, recovery, archival, and destruction; and
2) Cryptographic device lifecycle management events.

B. CA and Subscriber Certificate lifecycle management events, including:
1) EV Certificate Requests, renewal requests, re-key requests, and revocation;
2) Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
3) Acceptance and rejection of Certificate Requests;
4) Issuance of Certificates; and
5) Generation of Certificate Revocation Lists (CRLs) and OCSP entries.

C. Security events, including:
1) Successful and unsuccessful PKI system access attempts;
2) PKI and security system actions performed;
3) Security profile changes;
4) System crashes, hardware failures, and other anomalies;
5) Firewall and router activities; and
6) Entries to and exits from the Trustwave 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:

A. Network segregation
B. Network intrusion detection systems,
C. Network firewalls, and
D. 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.

A. 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;
B. All appropriate documentation submitted by Applicants in support of a Certificate application;
C. All records associated with Certificate issuance as part of its Certificate;
    1) Approval checklist process
    2) The Subscriber's PKCS#10 CSR;
    3) Documentation of organizational existence for organizational applicants as listed in Section 3.2.2;
    4) Documentation of Individual identity for Individual Applicants;
    5) Verification of organizational existence and status received from third party databases and government entities (including screen shots of web sites reporting such information);
    6) Screen shot of WHOIS record for domain name to be listed in the Certificate;
    7) Mailing address validation (if different than those identified through the resources listed above);
    8) Letter of authorization for web sites managed by third party agents of Applicants (if applicable);
    9) Submission of the Certificate application, including acceptance of the Subscriber Agreement;
    10) Name, e-mail, and IP address of person acknowledging authority of the Contract Signer and Approver;
    11) Other relevant contact information for the Applicant/Subscriber; and
    12) 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 at least 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:

A. Inform all subscribers and relying parties of which the Trustwave CA is aware.
B. 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:

A. Notify all subordinate CA's;
B. Make a reasonable effort to notify subscribers;
C. Immediately revoke all certificates issued within that portion of the TPH by issuing final CRL's for all certification authorities underneath the compromised certification authority, and subsequently terminate issuing and distribution of Certificates and CRL's;
D. Request revocation of the compromised Certificate; and

E. 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:

A. Trustwave IT Disaster Recovery Plan (current: version 3.0, October 2007)
B. Trustwave Business Continuity Plan (current: version 1.0, October 2007)
C. 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 practical, Trustwave will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

A. Provision of notice to parties affected by the termination, such as Subscribers and Relying Parties;
B. Informing such parties of the status of the CA;
C. Handling the cost of such notice;
D. The preservation of the CA's archives and records for the time periods required in this CP/CPS;
E. The continuation of Subscriber and customer support services;
F. The continuation of revocation services, such as the issuance of CRL's;
G. The revocation of unexpired, unrevoked Certificates of Subscribers and subordinate CAs, if necessary;
H. 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;
I. Disposition of the CA's Private Key and the hardware tokens containing such Private Key;
J. Provisions needed for the transition of the CA's services to a successor CA; and
K. 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 CP/CPS.

### 6.1.1 Key Pair Generation

#### *6.1.1.1 Trustwave Certification Authority Key Pair Generation*

All Trustwave owned and managed certification authority key pairs shall be:

A. Generated in hardware security modules as defined in section 6.2;
B. RSA key pairs generated on or before December 31, 2009 shall be of at least 2048 bit size. RSA key pairs generated on or after January 1, 2010 shall be of at least 4096 bit size;
C. 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
D. Performed by multiple trusted and qualified Trustwave employees.

*6.1.1.2 Subscriber key pair generation*

| Friendly Name | Certificate Policy ID | RSA Modulus Size |
|---|---|---|
| S/MIME Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.5.4.3.3 | 2048 |
| OV Code Signing Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.3.4 | 2048 |
| SUCA Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.5.3 | 2048 |
| ORGCA Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.4.4.4.3 | 2048 |
| Client Authentication Certificate, "My Identity" Certificate, VPN Certificate | 1.3.6.1.4.1.30360.3.3.3.5.4.6.3<br>1.3.6.1.4.1.30360.3.3.3.4.4.6.3 | 1024 |
| ISSL Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.7.3 | 1024 |
| EV Certificate | 2.16.840.1.114404.1.1.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.3 | 2048 |
| OV Certificate | 2.16.840.1.114404.2.1.2<br>2.16.840.1.114404.1.1.2.3.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.4.3 | 2048 |
| DV Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.5.3 | 2048 |
| Server All-Purpose Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.6.3 | 2048 |

Trustwave does not perform Subscriber key pair generation, except for (i) key pairs managed by Trustwave on behalf of independent organizations with the corresponding organization's certification authority certificates underneath ORGCA and (ii) key pairs that certain managed services clients may authorize and request Trustwave to manage. All other end 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 3 hardware security module.

### 6.1.2 Private Key Delivery to Subscriber

Trustwave does not perform private key 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 recommends that CSRs of Applicants use at least 1024 bit RSA keys. Trustwave may, at its discretion, not approve CSRs utilizing 512 bit or lower key size. Following December 31, 2009, Trustwave shall not accept CSR's for EV certificates of less than 2048 bit RSA keys.

### 6.1.6 Public Key Parameters Generation and Quality Checking

The public exponent of all root keys within the TPH shall use a public exponent of 3, 5, 17, or 65,537 for the generation of their RSA key pair. All hardware security modules used for storage of Trustwave managed certification authority keys shall be FIPS 186-3 compliant and shall provide hardware-based pseudo-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 keyUsage field so that the usage of the private key can be delimited and determined by X.509 compliant software. In addition, Subscriber Certificates may have extended key usage extensions set.

No Certificate within, or issued by any CA within, the TPH shall have the Non Repudiation ("nonRepudiation") extKeyUsage bit present within the certificate.

| *Friendly Name* | *Certificate Policy ID* | *keyUsages* |
|---|---|---|
| All Trustwave Subordinate CAs within the TPH | N/A | • KU: **Digital Signature, Certificate Signing, CRL Signing**<br>• EKU: None |
| S/MIME Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.5.4.3.3 | • KU; **Digital Signature, Key Encipherment**<br>• EKU: Secure Email |
| OV Code Signing Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.3.4 | • KU; **Digital Signature**<br>• EKU: **Code Signing** |

| | | |
|---|---|---|
| SUCA Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.5.3 | • KU: Any<br>• EKU: Any |
| ORGCA Certificate | 2.16.840.1.114404.2.2.1<br>1.3.6.1.4.1.30360.3.3.3.4.4.4.3 | • KU: **Certificate Signing, CRL Signing**<br>• EKU: None |
| Client Authentication Certificate, "My Identity" Certificate, VPN Certificate | 1.3.6.1.4.1.30360.3.3.3.5.4.6.3<br>1.3.6.1.4.1.30360.3.3.3.4.4.6.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Client Authentication** |
| ISSL Certificate | 1.3.6.1.4.1.30360.3.3.3.4.4.7.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication** |
| EV Certificate | 2.16.840.1.114404.1.1.2.4.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.3.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication** |
| OV Certificate | 2.16.840.1.114404.2.1.2<br>2.16.840.1.114404.1.1.2.3.1<br>1.3.6.1.4.1.30360.3.3.3.3.4.4.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication,** Client Authentication |
| DV Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.5.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication** |
| Server All-Purpose Certificate | 1.3.6.1.4.1.30360.3.3.3.3.4.6.3 | • KU: **Digital Signature, Key Encipherment**<br>• EKU: **Server Authentication, Client Authentication** |

## 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 3 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:

A. 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
B. 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

Trustwave maintains controls and procedures to provide reasonable assurance that Certificates and corresponding keys are valid for the applicable maximum period set forth below:

A. Root CA --31 years (XGCA, STCA, SGCA)
    a. All newly generated root CAs must be created with RSA modulus 4096 and must be set to expire no later than December 31, 2029, 2359.9999 hours.
B. Trustwave managed subordinate CA set to expire no later than December 31, 2029, 2359.9999 hours.
C. EV Certificates—27 months
D. EV and Non-EV Code Signing Certificates – 39 months
E. ORGCA certificates—10 years.
F. All other certificate types– 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

The Trustwave Information Security Program includes technical information security controls and performs regular risk assessments (Risk Assessments) that:

A. Identify reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any data or processes;
B. Assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of data and processes; and
C. Assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Trustwave CA has in place to control such risks

### 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 B)

### 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**

A. All certification authority Certificates shall include the basic constraints extension with a subject type equal to "CA" and its criticality set to "critical".
B. Subordinate CAs underneath ORGCA that are not managed by Trustwave shall have the path length constraint set to "0".
C. All basic constraints extensions within certification authority Certificates shall be marked as critical.

**Key Usage**

D. 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**

E. 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:

A. Trustwave's EV OID in the certificate policies extension. Trustwave's EV OID is 2.16.840.1.114404.1.1.2.4.1.
B. The basic Constraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. The key usage, marked as non-critical, set to include Signing and Key Encipherment.
D. 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.
E. 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.

F. The subject alternative name extension may be present.

*7.1.2.3 OV Web Server SSL Certificate extensions*

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

A. Trustwave's OV OID in the certificate policies extension. Trustwave's OV OID is 2.16.840.1.114404.2.1.2.
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. 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.
D. 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 the identifier defined in section 1.1 depending on the issuing CA.
E. The subject alternative name extension may be present.

*7.1.2.4 EV Code Signing Certificate Extensions*

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

A. 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.
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. The extended 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.
D. 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.
E. The subject alternative name extension may be present.

*7.1.2.5 OV Code Signing Certificate Extensions*

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

A. 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.
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity
C. The extended 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.

D. 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.
E. The subject alternative name extension may be present.

*7.1.2.6 Client Authentication Certificate Extensions*

All VPN client authentication Certificates issued by Trustwave to a Subscriber shall include:

A. Trustwave's client authentication OID in the certificate policies extension. Trustwave's client authentication OID is: 1.3.6.1.4.1.30360.3.3.3.5.4.6.3 or 1.3.6.1.4.1.30360.3.3.3.4.4.6.3 (prior to June 30, 2010);
B. The basicConstraints extension, marked as Critical, with Subject Type=End Entity;
C. The key usage extension set equal to digital signature and key encipherment
D. The extended key usage extension set equal to client authentication for both VPN client and server endpoints, and the extended key usage extension set equal to server authentication for VPN servers
E. The CRL Distribution Point extension, marked as non-critical, set equal to either http://crl.securetrust.com/CLACA.crl or http://crl.trustwave.com/CLACA.crl.
F. The subject alternative name extension may be present.

*7.1.2.7 Independent Organization Certification Authority Certificate Extensions*

All Certificates issued by Trustwave to an Independent Organization Certification Authority Subscriber shall include:

A. The independent organization's OID in the certificate policies extension for the certification practices statement applicable to the operation of the certification authority.
B. The basic Constraints extension, marked as Critical, with Subject Type=CA and Path Length Constraint=1
C. The CRL Distribution Point extension, marked as non-critical, set equal to http://crl.trustwave.com/XXXX.crl where XXXX represents an abbreviation of the independent organization.

Independent organizations utilizing certification authorities underneath ORGCA shall not include digital signature and non-repudiation indicators within the key usage extension, except with the written permission of Trustwave. Independent organization certification authority relying party agreements must clearly delineate and define the usage for the independent organization utilizing Certificates with digital signature or non-repudiation bits set within the key usage extension of any Subscriber. Unless the usage of digital signatures and non-repudiation key usage extensions are specifically permitted within the independent organization's relying party agreement and Certification Practices Statement, and approved by Trustwave, these End-Entity certificates shall not be utilized in any manner, including without limitation, to create any form of a legally

binding signature on a document or message in any jurisdiction. Typically, the use of digital signature and non-repudiation key usage extensions will be necessitated due to commercial-off-the- shelf software's reliance upon these extensions for their internal mechanisms.

*7.1.2.8 S/MIME Certificate Extensions*

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

A. Trustwave's S/MIME OID in the certificate policies extension. Trustwave's S/MIME OID is 2.16.840.1.114404.2.2.1 (prior to June 30, 2010) or 1.3.6.1.4.1.30360.3.3.3.5.4.3.3
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. The extendedKeyUsage, 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.
D. 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 the identifier defined in section 1.1 depending on the issuing CA.

*7.1.2.9 Internal SSL Certificate Extensions*

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

A. Trustwave's ISSL OID in the certificate policies extension. Trustwave's ISSL OID is 1.3.6.1.4.1.30360.3.3.3.4.4.7.3.
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. 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.
D. 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 the identifier defined in section 1.1 depending on the issuing CA.
E. The subject alternative name extension may be present.

*7.1.2.10 Domain Validation Certificate Extensions*

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

A. Trustwave's DV OID in the certificate policies extension. Trustwave's ISSL OID is 1.3.6.1.4.1.30360.3.3.3.3.4.5.3.
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. 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.

D. 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 the identifier defined in section 1.1 depending on the issuing CA.
E. The subject alternative name extension shall not be present.

*7.1.2.11 Server All-Purpose Certificate Extensions*

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

A. Trustwave's SAPCA certificate OID in the certificate policies extension. Trustwave's ISSL OID is 1.3.6.1.4.1.30360.3.3.3.3.4.6.3.
B. The basicConstraints extension, marked as Critical, with Subject Type=End-Entity and Path Length Constraint=None
C. The extended Key Usage, marked as non-critical, set equal to TLS Web Server Authentication (1.3.6.1.5.5.7.3.1) and TLS client authentication (1.3.6.1.5.5.7.3.2). No other values within the enhanced Key Usage extension shall be set.
D. 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 the identifier defined in section 1.1 depending on the issuing CA.
E. The subject alternative name extension may be present.

*7.1.2.12 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 owned and managed by Trustwave within the TPH, CRL's conforming to RFC 5280 shall be issued on a daily basis containing:

A. Version (set to "1" in order to indicate version 2);
B. Issuer Signature Algorithm (SHA-1 with RSA Encryption {1 2 840 113549 1 1 5});
C. Issuer Distinguished Name (the issuing certification authority);
D. This Update in ISO 8601 format with UTC designation.
E. Next Update in ISO 8601 format with UTC designation;
F. The list of revoked Certificates including reason code;
G. Serial Number;
H. Revocation Date;
I. 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:

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

## 7.3 OCSP Profile

Trustwave operates an OCSP service at http://ocsp.trustwave.com/. Trustwave's OCSP responders conform to version 1 of IETF RFC 2560.

### 7.3.1 Version Number(s)

OCSP responses issued by Trustwave shall use version 1 as defined within IETF RFC 2560.

### 7.3.2 OCSP Extensions

Appropriate extensions from the RFC 2560 may be used in OCSP requests and responses. If a request contains a nonce and the response does not contain the nonce, the Relying Party may process the response if the information is deemed reasonably current.

# 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

Trustwave and all components of the TPH SHALL:

A. Comply with applicable laws;

B. Comply with the requirements of this Certificate Policy and Certification Practice Statement; and

C. Comply with the requirements of the then-current WebTrust program for CAs v1.2 (or later) completed by a licensed WebTrust for CAs auditor or ETSI TS 102 042 V2.1.2 (or later). Trustwave conforms to the Lightweight Certificate Policy (LCP) and the Extended Validation Certificates Policy (EVCP) of ETSI TS 102 042 V2.1.2. Prior to issuance of any qualified certificate within the European Union community, Trustwave shall migrate all policy and practice to adhere to the extended Normalized Certificate Policy (NCP+).

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 (hereinafter, "Guidelines").

Material exceptions or deficiencies identified during an audit will result in a determination of actions to be taken. This determination is made by the independent auditor with input from the Trustwave management. 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, including extended validation criteria, on a yearly basis.

On a yearly basis, Trustwave shall conduct a review and/or audit of all third party entities performing Registration Authority activities for Trustwave. Circumstances and criteria for these yearly audits shall be defined within the contractual relationship between the third party and Trustwave, and approved by Trustwave management.

## 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:

A. Has no financial, business, or legal interest with Trustwave;
B. Has demonstrated proficiency and competence in regards to public key infrastructure technology; and is
C. 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:

A. CA business practices disclosure
B. Detailed validation process
C. Service integrity
D. 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.

## 8.7 Audit Requirements

### 8.7.1 Pre-Issuance Readiness Audi

A. If Trustwave has a currently valid WebTrust Seal of Assurance for CAs (is a currently valid unqualified opinion indicating compliance with equivalent audit procedures approved by the CA/Browser Forum), then before issuing EV Certificates the Trustwave and its Root CA MUST successfully complete a point-in –time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.
B. If Trustwave does ***not*** have a currently valid WebTrust Seal of Assurance for CAs (or currently valid unqualified opinion indicating compliance with equivalent audit procedures approved by the CA/Browser Forum), then before issuing EV Certificates Trustwave and its Root CA MUST successfully complete both: (i) a point –in-time readiness assessment audit against the WebTrust EV Program, or an equivalent for both (i) and (ii) as approved by the CA/ Browser Forum.

### 8.7.2 Regular Self Audits

During the period in which it issues EV Certificates, Trustwave MUST strictly control its service control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Certificates where the final cross correlation and sue diligence requirements of Section 24 of these Guidelines is performed by an RA, Trustwave MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

### 8.7.3 Annual Independent Audit

During the period in which it issues EV Certificates, Trustwave and its Root CA Must undergo and pass an annual (i) WebTrust Program for CAs audit and (ii)WebTrust EV Program audit, or an equivalent for both (i) and (ii) as approved by the CA/Browser Forum. Such audits MUST cover all CA obligations under these Guidelines regardless of whether they are performed directly by the Trustwave CA or delegated to an RA or subcontractor.

### 8.7.4 Auditor Qualifications

All audits required under these Guidelines MUST be performed by a Qualified Auditor. A Qualified Auditor MUST:

A. Be an independent public accounting firm that has proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function and be currently licensed to perform WebTrust for CA audits and WebTrust EV Program audits, or to perform such alternate equivalent audits approved by the CA/Browser Forum as will be performed; and
B. Be a member of the American Institute of Certified Public Accountants (AICPA), or a non-US equivalent that requires that audits be completed under defined standards that include the possession of certain skill sets, quality assurance measures such as peer review , competency testing, standards with respect to proper assignment of staff to engagements, and requirements for continuing professional education; and
C. Maintain Professional Liability/Errors &Omissions insurance, with policy limits of at least $1 million in coverage.

### 8.7.5 Root Key Generation

For CA Root keys, Trustwave's Qualified Auditor SHOULD witness the root key generation ceremony in order to observe the process and the controls over the integrity and confidentiality of the Trustwave CA root keys produced. The Qualified Auditor MUST then issue a report opining that Trustwave, during its root key and certificate generation process:

A. Documented its Root CA key generation and protection and procedures in its Certificate Policy, and its Certification Practices Statement, (CP and CPS);
B. Included appropriate detailed procedures and controls in a documented plan of procedures to be performed for the generation of the root certification authority key pair (the "Root Key Generation Script") for the Root CA;
C. Maintained effective controls to provide reasonable assurance that the Root CA was generated and protected in conformity with the procedures required by its Root Key Generation Script.
D. A video of the entire key generation ceremony SHALL be recorded.

# 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 CP/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.

A. CA application records, whether approved or disapproved;
B. Certificate Application records;
C. Subscriber Agreement
D. Private keys held by customers and subscribers and information needed to recover such Private Keys;
E. Transactional records;
F. Contingency planning and disaster recovery plans; and
G. 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:

A. Certificates;
B. Certificate revocation;
C. Certificate status; and
D. Trustwave repositories and their contents.

### 9.3.3 Responsibility to Protect Confidential Information

Trustwave protects and secures confidential information from disclosure.

### 9.3.4 Privacy Plan

Trustwave's privacy plan/policy may be found at the following location: https://www.trustwave.com/downloads/Trustwave-Privacy-Policy.pdf.

### 9.3.5 Information Treated as Private

Non-public Subscriber information is treated as private.

### 9.3.6 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.

### 9.3.7 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.

### 9.3.8 Notice and Consent to Use Private Information

Unless otherwise stated in this CP/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.

#### 9.3.9 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.

#### 9.3.10 Other Information Disclosure Circumstances

Refer to section 9.4.6.

## 9.4 Intellectual Property Rights

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

A. This CPS and CPs;
B. Certificates;
C. Revocation Information;
D. Trustwave's logos, trademarks and service marks; and
E. Trustwave's roots keys and the root Certificates containing them.

## 9.5 Representations and Warranties

#### 9.5.1 CA Representations and Warranties

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

A. there are no material misrepresentations of fact with the Certificates;
B. 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;
C. the Certificates comply with the material requirements of this CPS and the applicable CPs; and
D. Trustwave's revocation services and its repositories materially comply with this CPS and the applicable CPs.

#### 9.5.2 RA Representations and Warranties

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

A. there are no material misrepresentations of fact with the Certificates;
B. 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;
C. the Certificates comply with the material requirements of this CPS and the applicable CPs; and
D. Trustwave's revocation services, if applicable, and its repositories materially comply with this CPS and the applicable CPs.

#### 9.5.3 Subscriber Representations and Warranties

Subscribers warrant that:

A. 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;

B. Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key;
C. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
D. All information supplied by the Subscriber and contained in the Certificate is true;
E. The Certificate is being used exclusively for authorized and legal purposes consistent with this CP/CPS, and
F. 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.
G. No subscriber private key associated with any certificate issued within the Trustwave public key infrastructure, with the exception of those certificates issued by the Trustwave document certification authority, shall be used to affix a digital signature to any document, contract, or letter.

Subscriber Agreements may include additional representations and warranties.

#### 9.5.4 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 CP/CPS.

In no event shall a Relying Party construe a signature affixed to any document or message, that has been created utilizing a private key corresponding to a Trustwave issued certificate, as legally binding.

Relying Party Agreements may include additional representations and warranties.

## 9.6 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 CP/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 CP/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 CPs. 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

## 9.7 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 CP/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.

## 9.8 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 CP/CPS and the Relying Party Agreement, including without limitation the Relying Party's (i) failure to verify a Certificate in accordance with this CP/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.

## 9.9 Term and Termination

### 9.9.1 Term

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

### 9.9.2 Termination

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

#### 9.9.3 Effect of Termination and Survival

Upon Termination of this CPS or the applicable CPs, 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.

### 9.10 Individual Notices and Communications with Participants

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

### 9.11 Amendments

#### 9.11.1 Procedure for Amendment

Refer to Section 1.5.4 hereof.

#### 9.11.2 Notification Mechanism and Period

Trustwave reserves the right to amend this CPS and the applicable CPs 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 CPs shall be posted in Trustwave's repository. Such publication shall serve as notice to all relevant entities.

#### 9.11.3 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.

### 9.12 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 CPs, 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 CPs 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.

## 9.13 Governing Law

The enforceability, construction, interpretation, and validity of this CPS, the applicable CPs 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.

## 9.14 Compliance with Applicable Law

This CPS and the applicable CPs 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

## 9.15 Miscellaneous Provisions

### 9.15.1 Entire Agreement

This CPS, the applicable CPs, 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.

### 9.15.2 Assignment

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

### 9.15.3 Severability

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

### 9.15.4 Enforcement (Attorneys' Fees and Waiver of Rights)

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

### 9.15.5 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.

## 9.16 Other Provisions

No stipulation.

# 10 APPENDIX A – REFERENCES


A. ETSI TS 102 042 V2.1.2, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
B. FIPS 140-2 Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.
C. RFC2119 Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
D. RFC2527 Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
E. RFC3546 Request for Comments: 3546, Transport Layer Security (TLS) Extensions, Blake-Wilson et al, June 2003.
F. RFC3647 Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani et al, November 2003.
G. RFC3739 Request for Comments: 3739, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, Santesson et al, March 2004.
H. RFC5280 Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
I. WebTrust WebTrust for Certification Authorities – Extended Validation audit criteria, Canadian Institute of Chartered Accountants, 2009.
J. X.509v3 ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.


# 11 APPENDIX B – TRUSTWAVE GLOBAL ROOT CERTIFICATES

## 11.1 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-----

## 11.2 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-----


## 11.3 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-----