CERTIFICATE POLICY AND CERTIFICATION PRACTICES STATEMENT
VERSION 6.6
MAY 26, 2021

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

- 1.3.6.1.4.1.30360.3.3.3,
- 2.16.840.1.114404, and
- 2.23.140.1

Certificate Policy and Certification Practices Statement

This document defines “Certification Practice” and “Certificate Policy” for all publicly-trusted Certificate Authorities and Digital Certificates issued by SecureTrust, a division of Trustwave Holdings, Inc. (hereinafter, “SecureTrust”). All Digital Certificates being issued by SecureTrust 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 SecureTrust 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	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	2.23.140.1.4.1
3. 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
4. Extended Validation (“EV”) Web Server SSL Digital Certificate	EV Certificate	2.16.840.1.114404.1.1.2.4.1, 2.23.140.1.1
5. Organization Validation (“OV”) Web Server SSL Digital Certificate	OV SSL Certificate	2.23.140.1.2.2, 2.23.140.1.2.3
6. Domain Validation (“DV”) Web Server SSL Digital Certificate	DV Certificate	2.23.140.1.2.1
7. Timestamp Certificate	Timestamp Certificate	1.3.6.1.4.1.30360.3.3.3.3.4.8.3

Table 1

SecureTrust, a Trustwave division

CERTIFICATION PRACTICES AND CERTIFICATE POLICY STATEMENT

Trademark Notices

The SecureTrust logo and design, Trustwave, SecureTrust, and XRamp are trademarks and/or service marks of Trustwave Holdings, Inc. Other trademarks and service marks in this document are the property of their respective owners.

Without limiting the rights reserved above, and except as licensed below, no part of this publication may be reproduced, stored in or introduced into a retrieval system, or transmitted, in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), without prior written permission of Trustwave Holdings, Inc.'s, (hereinafter, "Trustwave") Legal Department.

Notwithstanding the above, permission is granted to reproduce and distribute this Certification Practices Statement and the associated Certificate Policies on a nonexclusive, royalty-free basis, provided that (i) the foregoing copyright notice and the beginning paragraphs are prominently displayed at the beginning of each copy, and (ii) this document is accurately reproduced in full, complete with attribution of the document to Trustwave.

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 600
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 ***SecureTrust Certificate Policy and Certification Practices Statement*** ("SecureTrust CP/CPS") which details the following information:

1. The legal and technical principles and practices that SecureTrust employs in providing certification services;
2. The governing policies, practices, procedures, and infrastructure employed by the SecureTrust Certification Authority ("CA") for its operations and business continuity;
3. The governing policies, practices and procedures employed in the creation, management, and termination of our root CA keys;
4. The governing policies, practices and procedures that apply to all End-Entity Digital Certificates ("Certificate") issued by our CA;
5. The physical, environmental, and logical security controls employed by SecureTrust to protect our root CA certificates and keys; and
6. The legal structure of the relationship between SecureTrust, Subscribers (end-entities), and Relying Parties.

Previous versions of this document were known as the ***Trustwave Certificate Policy and Certification Practices Statement***.

SecureTrust 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 SecureTrust, 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 SecureTrust 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 SecureTrust 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 SecureTrust 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://certs.securetrust.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 SecureTrust.

SecureTrust conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" and "Guidelines For The Issuance And Management Of Extended Validation Certificates" (henceforth referred to as "EV Guidelines") published at https://www.cabforum.org/. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

SecureTrust conforms to the current version of the "Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates" published at https://aka.ms/csbr. If there is any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.1 OVERVIEW

SecureTrust operates and maintains six distinct Root Certification Authorities (hereinafter, collectively known as “Root CA”, or “SecureTrust Root CA”) identified by the following names:

1. Secure Global Certification Authority (“SGCA”)
2. XRamp Global Certification Authority (“XGCA”)
3. SecureTrust Certification Authority (“STCA”)
4. Trustwave Global Certification Authority (“TWGCA”)
5. Trustwave Global ECC P256 Certification Authority (“TWGP256CA”)
6. Trustwave Global ECC P384 Certification Authority (“TWGP384CA”)

In addition, SecureTrust maintains subordinate CAs (hereinafter known as “SecureTrust 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 *“**SecureTrust Public Key Infrastructure Hierarchy**”* (“SPH”).

1. **SecureTrust Secure Email CA (“STSMCA”)**: This CA issues Certificates for S/MIME (secure email) use.
2. **Trustwave S/MIME Certification Authority SHA256 (“SMCA2”)**: This CA issues Certificates for S/MIME (secure email) use.
3. **SecureTrust TWG Secure Email CA (“TWGSMCA”)**: This CA issues Certificates for S/MIME (secure email) use.
4. **SecureTrust TWG ECDSA P-256 Secure Email CA (“TWGP2SMCA”)**: This CA issues Certificates for S/MIME (secure email) use.
5. **SecureTrust TWG ECDSA P-384 Secure Email CA (“TWGP3SMCA”)**: This CA issues Certificates for S/MIME (secure email) use.
6. **SecureTrust TWG Client CA (“TWGCLCA”)**: This CA issues “My Identity” client Certificates to be used for authentication purposes within a Virtual Private Network (“VPN”).
7. **SecureTrust TWG ECDSA P-256 Client CA (“TWGP2CLCA”)**: This CA issues “My Identity” client Certificates to be used for authentication purposes within a Virtual Private Network (“VPN”).
8. **SecureTrust TWG ECDSA P-384 Client CA (“TWGP3CLCA”)**: This CA issues “My Identity” client Certificates to be used for authentication purposes within a Virtual Private Network (“VPN”).
9. **SecureTrust Code Signing CA (“STCSCA”)**: This CA issues Certificates for code signing use.
10. **Trustwave Code Signing Certification Authority SHA256 (“CSCA2”)**: This CA issues Certificates for code signing use.
11. **Trustwave Global Code Signing CA (“TWGCSCA”)**: This CA issues Certificates for code signing use.
12. **Trustwave Global ECDSA P-256 Code Signing CA (“TWGP2CSCA”)**: This CA issues Certificates for code signing use.
13. **Trustwave Global ECDSA P-384 Code Signing CA (“TWGP3CSCA”)**: This CA issues Certificates for code signing use.
14. **SecureTrust Client Authentication CA (“STCLCA”)**: This CA issues “My Identity” client Certificates to be used for authentication purposes within a Virtual Private Network (“VPN”).
15. **Trustwave Client Authentication SHA256 CA (“CLACA2”)**: This CA issues “My Identity” client Certificates to be used for authentication purposes within a Virtual Private Network (“VPN”).
16. **SecureTrust Extended Validation CA (“STEVCA”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.
17. **Trustwave Extended Validation Certification Authority SHA256 (“EVCA2”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.
18. **Trustwave Secure Global Extended Validation CA (“SGEVCA”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.
19. **Trustwave XRamp Global Extended Validation CA (“XGEVCA”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.
20. **Trustwave Global Extended Validation CA (“TWGEVCA”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.
21. **Trustwave Global ECDSA P-256 Extended Validation CA (“TWGP2EVCA”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.
22. **Trustwave Global ECDSA P-384 Extended Validation CA (“TWGP3EVCA”)**: This CA issues EV Certificates for server (e.g. WWW server) implementations.

23. **SecureTrust Organization Validation CA ("STOVCA")**: This CA issues OV SSL Certificates for server (e.g. WWW server) implementations.
24. **Trustwave Organization Validation Certification Authority SHA256 ("OVCA2")**: This CA issues OV SSL Certificates for server (e.g. WWW server) implementations.
25. **Trustwave Global Organization Validation CA ("TWGOVCA")**: This CA issues OV Certificates for server (e.g. WWW server) implementations.
26. **Trustwave Global ECDSA P-256 Organization Validation CA ("TWGP2OVCA")**: This CA issues OV Certificates for server (e.g. WWW server) implementations.
27. **Trustwave Global ECDSA P-384 Organization Validation CA ("TWGP3OVCA")**: This CA issues OV Certificates for server (e.g. WWW server) implementations.
28. **SecureTrust Domain Validation CA ("STDVCA")**: This CA issues DV Certificates for server (e.g WWW server) implementations.
29. **Trustwave Domain Validation Certification Authority SHA256 ("DVCA2")**: This CA issues DV Certificates for server (e.g. WWW server) implementations.
30. **Trustwave Global Domain Validation CA ("TWGDVCA")**: This CA issues DV Certificates for server (e.g. WWW server) implementations.
31. **Trustwave Global ECDSA P-256 Domain Validation CA ("TWGP2DVCA")**: This CA issues DV Certificates for server (e.g. WWW server) implementations.
32. **Trustwave Global ECDSA P-384 Domain Validation CA ("TWGP3DVCA")**: This CA issues DV Certificates for server (e.g. WWW server) implementations.
33. **SecureTrust Timestamping CA ("STTSCA")**: This CA issues Timestamp Certificates for providing proof that code or other data existed at a given point in time. These Timestamp Certificates are controlled by SecureTrust and used to provide Trusted Timestamping services.
34. **Trustwave Timestamping CA ("TSCA")**: This CA issues Timestamp Certificates for providing proof that code or other data existed at a given point in time. These Timestamp Certificates are controlled by SecureTrust and used to provide Trusted Timestamping services.
35. **Trustwave Global Timestamping CA ("TWGTSCA")**: This CA issues Timestamp Certificates for providing proof that code or other data existed at a given point in time. These Timestamp Certificates are controlled by SecureTrust and used to provide Trusted Timestamping services.
36. **Trustwave Global ECDSA P-256 Timestamping CA ("TWGP2TSCA")**: This CA issues Timestamp Certificates for providing proof that code or other data existed at a given point in time. These Timestamp Certificates are controlled by SecureTrust and used to provide Trusted Timestamping services.
37. **Trustwave Global ECDSA P-384 Timestamping CA ("TWGP3TSCA")**: This CA issues Timestamp Certificates for providing proof that code or other data existed at a given point in time. These Timestamp Certificates are controlled by SecureTrust and used to provide Trusted Timestamping services.

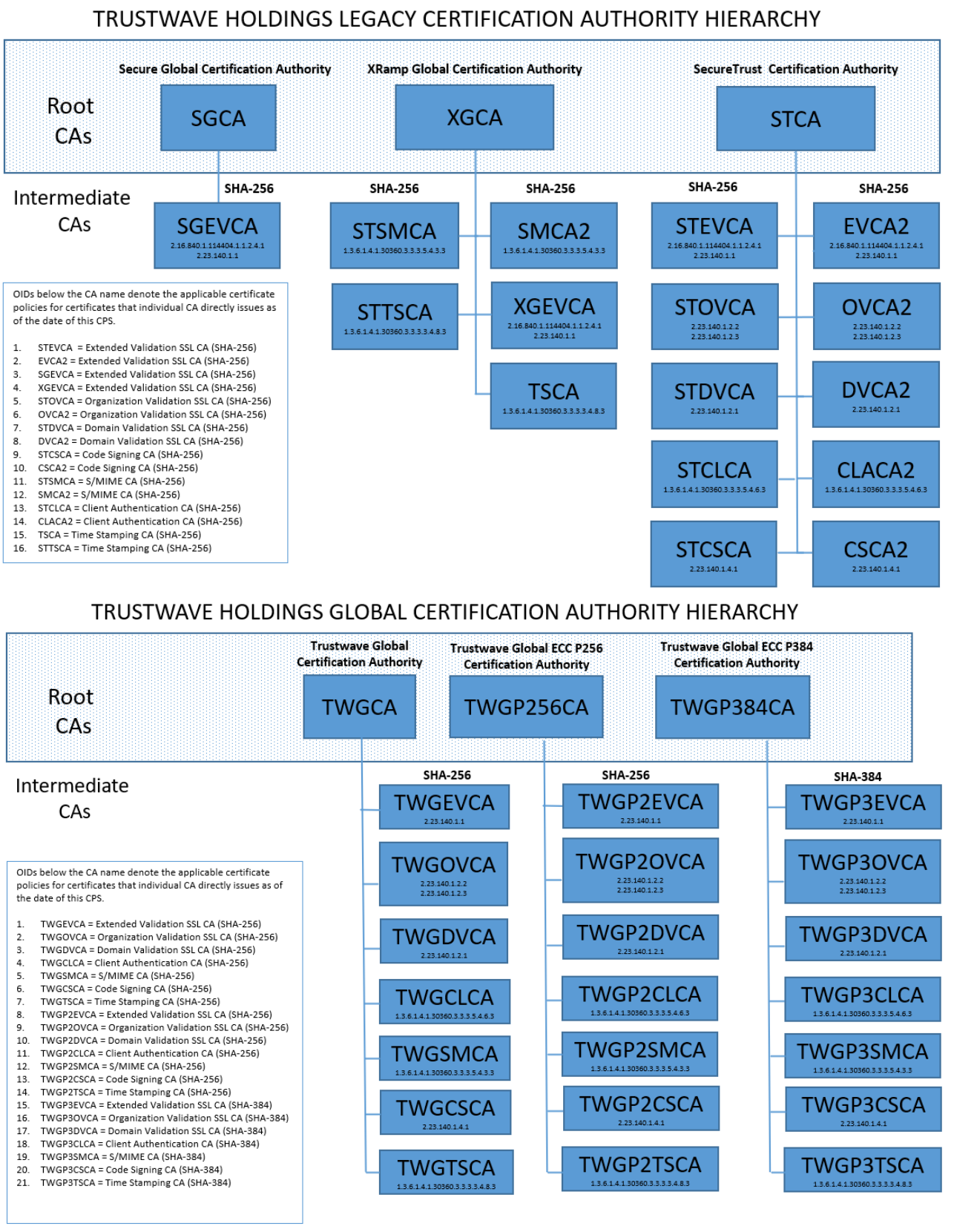

Figure 1 - The SecureTrust Public Key Infrastructure

Activities and governing policies of the SPH 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 SecureTrust are not defined within this document.

All End-Entity Certificates issued by SecureTrust 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:

1. Reviewing their Certificate as issued by SecureTrust to confirm the accuracy of the Subscriber information contained therein before first use,
2. Using a trusted system for generating their Key Pair and to prevent any loss, disclosure, or unauthorized use of the Private Key,
3. Keeping Private Keys confidential at all times,
4. Keeping confidential any passwords, pass-phrases, PINs or other personal secrets used in obtaining authenticated access to their Private Key and SecureTrust PKI facilities,
5. 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,
6. In accordance with the SecureTrust CP/CPS, exclusively using their Certificate for legal purposes and restricting its use to authorized purposes detailed by this document, and
7. Immediately notifying SecureTrust of a suspected or known Key Compromise in accordance with the procedures laid down in this SecureTrust CP/CPS.

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

1. Ensuring that reliance on Certificates issued under this policy is restricted to appropriate uses as defined within this SecureTrust CP/CPS,
2. Ensuring that the Certificate remains valid and has not been revoked by accessing any and all relevant certificate status information, and
3. 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://certs.securetrust.com/CA.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the ***SecureTrust Certificate Policy and Certification Practices Statement*** (“SecureTrust CP/CPS”).

All Certificates that SecureTrust 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.

SecureTrust 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. Table 2 below identifies any valid certificate type.

Certificate Type	Friendly Name	Issuing Certification Authority	Certificate Policy OID
Email S/MIME Digital Certificate	S/MIME Certificate, Secure E-Mail Certificate	STSMCA, SMCA2, TWGSMCA, TWGP2SMCA, TWGP3SMCA	1.3.6.1.4.1.30360.3.3.3.5.4.3.3
Organization Validation (“OV”) Code Signing Certificate	OV Code Signing Certificate	STCSCA, CSCA2, TWGCSCA, TWGP2CSCA, TWGP3CSCA	2.23.140.1.4.1
Client Authentication Certificate	Client Authentication Certificate, “My Identity” Certificate, VPN Certificate	STCLCA, CLACA2, TWGCLCA, TWGP2CLCA, TWGP3CLCA	1.3.6.1.4.1.30360.3.3.3.5.4.6.3
Extended Validation (“EV”) Web Server SSL Digital Certificate	EV Certificate	STEVCA, EVCA2, SGEVCA, XGEVCA, TWGEVCA, TWGP2EVCA, TWGP3EVCA	2.16.840.1.114404.1.1.2.4.1, 2.23.140.1.1
Organization Validation (“OV”) Web Server SSL Digital Certificate	OV SSL Certificate	STOVCA, OVCA2, TWGOVCA, TWGP2OVCA, TWGP3OVCA	2.23.140.1.2.2, 2.23.140.1.2.3
Domain Validation (“DV”) Web Server SSL Digital Certificate	DV Certificate	STDVCA, DVCA2, TWGDVCA, TWGP2DVCA, TWGP3DVCA	2.23.140.1.2.1
Timestamp Certificate	Timestamp Certificate	STTSCA, TSCA, TWGTSCA, TWGP2TSCA, TWGP3TSCA	1.3.6.1.4.1.30360.3.3.3.3.4.8.3

Table 2

1.2.1 Revisions

VERSION	CPB APPROVAL & PUBLICATION DATE	CHANGES/COMMENTS	MODIFIED BY
3.0	July 11, 2014	General Review & Annual Update	Sr. Product Manager, Software Architect, Director of Operations
3.1	August 20, 2014	Organization Updates	Director of Operations
4.0	October 1, 2014	Intermediate Roots	Director of Operations
4.1	December 15, 2014	Quarterly Update	Sr. Product Manager, Director of Operations
4.2	April 15, 2015	Quarterly Update	Director of Operations
4.3	August 12, 2015	Quarterly Update, Created 2 EV CAs, Revoked 2 unused CAs	Sr. Product Manager
4.4	January 14, 2016	CRL updates, Quarterly CPS update	Sr. Product Manager, Sr. Software Architect
4.5	June 22, 2016	Quarterly CPS Updates, Revoked and removed ORGCA, Validation Updates	Director Product Management, Sr. Software Architect
4.6	January 25, 2017	CPS Updates, Added TSCA	Director, Product Management, Sr. Software Architect, Associate Product Manager
4.7	April 19, 2017	CPS Updates, Validation Updates	Sr. Software Architect, Associate Product Manager
4.8	August 23, 2017	CAA Policy Update, Instances of “OV Certificate” changed to “OV SSL Certificate”, Revocation request clarification, Non-Latin Organization name coding no longer EV only and change to RFC references, Organization Updates, Added ECDSA key requirements	Software Architect, Associate Product Manager
5.0	January 31, 2018	New roots added, Certificate Transparency updates, New Certificate duration requirements, Various clarity updates as identified by the annual review	Software Architect, Associate Product Manager
5.1	October 1, 2018	Removed unused definitions and acronyms, Deprecation of method 3.2.2.4.1, Clarified 3.2.2.5, Removal of outdated ETSI versions, Clarified insurance coverage 9.2.1	Software Architect, Associate Product Manager
5.2	November 14, 2018	Removed unused definitions and acronyms, OCSP clarifications, Revocation updates, Various clarity updates	Software Architect, Associate Product Manager
6.0	April 24, 2019	Reformatted CPS, Added new intermediates, Completed SecureTrust rebranding, Replaced no stipulation sections, Added new domain validation methods 3.2.2.4.13-3.2.2.4.16, Removed domain validation 3.2.2.4.3, Added securetrust.com as a CAA identifier	Software Architect, Associate Product Manager
6.1	March 18, 2020	Update section names to match RFC 3647, Remove revoked CSCA intermediate, Update used DV methods (set 3.2.2.4.6 deprecation date, clarify that 3.2.2.4.17 is not used, add 3.2.2.4.18-19), Various clarity updates	Software Architect, Product Manager
6.2	July 15, 2020	Clarity updates, Document compliance with Mozilla Root Policy, Update Policy Authority name, Update EV, OV SSL, and DV certificate lifetimes	Software Architect, Lead QA Engineer, Product Manager

VERSION	CPB APPROVAL & PUBLICATION DATE	CHANGES/COMMENTS	MODIFIED BY
6.3	September 23, 2020	Subscriber Certificate revocation clarification, Update PKI hierarchy, Add EV data source	Software Architect, Lead QA Engineer, Product Manager
6.4	October 21, 2020	Add certificate problem reporting email address	Software Engineer, Product Manager
6.5	April 29, 2021	Add requirement for proof of key compromise	Software Engineer, Product Manager
6.6	May 26, 2021	Update DV methods 18 and 19, for ballot SC44	Software Engineer, Product Manager

1.3 PKI PARTICIPANTS

1.3.1 Certification Authorities

All Certification Authorities that are listed in section 1.1 are governed by this document and shall implement all requirements as listed within this statement.

1.3.2 Registration Authorities

SecureTrust may contract with Delegated Third Parties to service foreign markets by performing various RA functions under this CP/CPS. A business entity that is located in a foreign market and serves as an RA for SecureTrust 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. RAs will perform their functions in accordance with this CP/CPS, the relevant CPs, meet the qualification requirements in section 5.3.1, retain documentation in accordance with section 5.5.2, abide by the other provisions in the CA/Browser Forum Baseline Requirements that are applicable to the delegated function and the terms of their enterprise services agreement with SecureTrust. RAs may, in their discretion, prescribe more restrictive practices. Furthermore, SecureTrust shall perform a review and/or audit of all third party Registration Authority activities on a yearly basis.

SecureTrust shall not enter into agreements with a third party to act as a Registration Authority with EV SSL or OV code signing Certificate issuance or to perform Domain Validation functions as described in sections 3.2.2.4 and 3.2.2.5. SecureTrust shall not delegate the validation of control for email addresses when processing requests for S/MIME Certificates.

In addition, SecureTrust may contract with Enterprise RAs to verify Certificate requests for the Enterprise RA's own organization. SecureTrust will not accept Certificate requests from Enterprise RA's unless SecureTrust has confirmed that the requested FQDN is within the Enterprise RA's verified Domain Namespace. If the subject name requested is other than an FQDN, the name would be confirmed as that of the institution, or an Affiliate of the institution, or that the institution is an agent of the named organization.

1.3.3 Subscribers

SecureTrust 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 SecureTrust. 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 SecureTrust or 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 SecureTrust 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 SecureTrust PKI are SecureTrust, 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 SecureTrust 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 keyUsage 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.)

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

SecureTrust 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, SecureTrust issues many different types of Certificates, which are all intended for different purposes. The following table lists all certificate types that are issued by SecureTrust. The general description for each type’s permissible use is given within the following table:

Friendly Name	Certificate Policy ID	keyUsages	extendedKeyUsages	Description
1. All SecureTrust Subordinate CAs within the SPH	All	**Digital Signature, Certificate Signing, CRL Signing**	One or more of **Client Authentication, Server Authentication, Code Signing, Secure Email, Time Stamping**	The Certificate defining any CA operated by SecureTrust, 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, and 3) sign OCSP responses that are applicable to its issued Certificate population.
2. S/MIME Certificate	1.3.6.1.4.1.30360.3.3.3.5.4.3.3	**Digital Signature, Key Encipherment** (optional)	**Secure Email (1.3.6.1.5.5.7.3.4)**	The SecureTrust S/MIME Certificate that is issued to subscribers, along with its associated Private Key, shall be used only to enable secure email communication.
3. OV Code Signing Certificate	2.23.140.1.4.1	**Digital Signature**	**Code Signing (1.3.6.1.5.5.7.3.3)**	The SecureTrust OV code signing Certificate as issued to Subscribers, along with its associated Private Key, shall be used only to digitally sign application code.
4. Client Authentication Certificate, “My Identity” Certificate, VPN Certificate	1.3.6.1.4.1.30360.3.3.3.5.4.6.3	**Digital Signature, Key Encipherment**	**Client Authentication (1.3.6.1.5.5.7.3.2)**	These Certificates shall be used only to enable client authentication within virtual private network construction. These certificates are issued to individuals for the purpose of a VPN authentication and tunnel construction.
5. EV Certificate	2.16.840.1.114404.1.1.2.4.1 2.23.140.1.1	**Digital Signature, Key Encipherment** (optional)	**Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)**	SecureTrust EV Certificates shall be used only to enable TLS (SSL) communication between server and client endpoints.
6. OV SSL Certificate	2.23.140.1.2.22.23.140.1.2.3	**Digital Signature, Key Encipherment** (optional)	**Server Authentication (1.3.6.1.5.5.7.3.1), Client Authentication (1.3.6.1.5.5.7.3.2)**	SecureTrust OV SSL Certificates shall be used only to enable TLS (SSL) communication between server and client endpoints.

Friendly Name	Certificate Policy ID	keyUsages	extendedKeyUsages	Description
7. DV Certificate	2.23.140.1.2.1	**Digital Signature, Key Encipherment** (optional)	EKU: **Server Authentication (1.3.6.1.5.5.7.3.1)**	SecureTrust DV Certificates shall be used only to enable TLS (SSL) communication between server and client endpoints.
8. Timestamp Certificate	1.3.6.1.4.1.30360.3.3.3.3.4.8.3	**Digital Signature**	**Time Stamping (1.3.6.1.5.5.7.3.8)**	SecureTrust Timestamp Certificates shall be issued only to SecureTrust, a division of Trustwave, and used only to provide Trusted Timestamps for code and data.

Table 3

1.4.2 Prohibited Certificate Uses

As a general rule, **no Certificate issued by SecureTrust shall possess or be recognized as possessing the capability of digitally signing any type of document (contract, legal letter, etc.).**

Certificates issued by SecureTrust 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 SecureTrust-issued Certificate where the use or intended use by a Relying Party is not defined within this document.

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

1. That the Subject named in the Certificate is actively engaged in doing business;
2. That the Subject named in the Certificate complies with applicable laws;
3. That the Subject named in the Certificate is trustworthy, honest, or reputable in its business dealings; or
4. That it is "safe" to do business with the Subject named in the Certificate.

SecureTrust 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.

SecureTrust Certificates shall not be used for the interception of encrypted communications ("man-in-the-middle").

SecureTrust 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 Section 4.5.1. SecureTrust 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. SecureTrust does not warrant any use of

Intermediate CAs as root Certificates. Upon a re-key event, Subscribers must cease reliance upon the old keys. SecureTrust 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 600
Chicago, Illinois 60602
USA

1.5.2 Contact Persons

SecureTrust CA Operational Committee
70 West Madison Street, Suite 600
Chicago, Illinois 60602
USA

Email: sslsupport@trustwave.com

Subscribers, Relying Parties, Application Software Suppliers, and other third parties shall contact SecureTrust at cert-problem-report@securetrust.com to report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

1.5.3 Person Determining CPS Suitability for the Policy

SecureTrust's Certification Practice Board ("CPB") 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 senior leadership of Trustwave.

1.5.4 CPS Approval Procedures

All changes and revisions to this CPS and the related CPs shall be approved by the CPB. The CPB meets periodically but also has the ability for emergency meetings when necessary. Changes to this CPS can be based on, but not limited to, any of the following:

- Industry regulation changes
- Technical changes to the CA infrastructure
- Business changes

Potential CPS changes are identified by the CA Operational Committee and presented to the CPB for review. The CA Operational Committee performs a complete CP/CPS review at least on an annual basis.

SecureTrust reserves the right to amend this document in its discretion from time to time. Additionally, SecureTrust will update this document at least annually, even if there are no substantive changes.

All amendments and updates shall be posted in SecureTrust's repository located at https://certs.securetrust.com/CA.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

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 or Legal Entity that applies for (or seeks renewal of) a Certificate. Once the Certificate issues, the Applicant is referred to as the Subscriber. For Certificates issued to devices, the Applicant is the entity that controls or operates the device named in the Certificate, even if the device is sending the actual certificate request.

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 SecureTrust.

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

Attestation Letter: A letter attesting that subject information is correct written by an accountant, lawyer, government official, or other reliable third party customarily relied upon for such information.

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

Authorization Domain Name: The Domain Name used to obtain authorization for certificate issuance for a given FQDN. The CA may use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN starts with a wildcard character, then the CA MUST remove all wildcard labels from the left most portion of requested FQDN. The CA may prune zero or more labels from left to right until encountering a Base Domain Name and may use any one of the intermediate values for the purpose of domain validation.

Authorized Port: One of the following ports: 80 (http), 443 (https).

Base Domain Name: The portion of an applied-for FQDN that is the first domain name node left of a registry- controlled or public suffix plus the registry-controlled or public suffix (e.g. “example.co.uk” or “example.com”). For FQDNs where the right-most domain name node is a gTLD having ICANN Specification 13 in its registry agreement, the gTLD itself may be used as the Base Domain Name.

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 Problem Report: Complaint of suspected Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, or inappropriate conduct related to Certificates.

Certificate Requester: 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.

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

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

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 that is used to establish a trust relationship between two Root CAs.

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.

DNS CAA Email Contact: The email address defined in section B.1.1 of the CA/Browser Forum Baseline Requirements.

DNS TXT Record Email Contact: The email address defined in section B.2.1 of the CA/Browser Forum Baseline Requirements.

DNS TXT Record Phone Contact: The email address defined in section B.2.2 of the CA/Browser Forum Baseline Requirements.

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.

Domain Authorization Document: Documentation provided by, or a CA’s documentation of a communication with, a Domain Name Registrar, the Domain Name Registrant, or the person or entity listed in WHOIS as the Domain Name Registrant (including any private, anonymous, or proxy registration service) attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace.

Domain Contact: The Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

Domain Name: The label assigned to a node in the Domain Name System.

Domain Namespace: The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.

Domain Name Registrant: Sometimes referred to as the “owner” of a Domain Name, but more properly the person(s) or entity(ies) registered with a Domain Name Registrar as having the right to control how a Domain Name is used, such as the natural person or Legal Entity that is listed as the “Registrant” by WHOIS or the Domain Name Registrar.

Domain Name Registrar: A person or entity that registers Domain Names under the auspices of or by agreement with: (i) the Internet Corporation for Assigned Names and Numbers (ICANN), (ii) a national Domain Name authority/registry, or (iii) a Network Information Center (including their affiliates, contractors, delegates, successors, or assigns).

End-Entity: 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.

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

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

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

Extended Validation Certificate: See EV Certificate.

Fully-Qualified Domain Name: A Domain Name that includes the labels of all superior nodes in the Internet Domain Name System.

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 Certificate Request: A Request that SecureTrust flags for additional scrutiny which may include names at higher risk for phishing or other fraudulent usage.

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.

Individual: A natural person.

Internal Name: A string of characters (not an IP address) in a Common Name or Subject Alternative Name field of a Certificate that cannot be verified as globally unique within the public DNS at the time of certificate issuance because it does not end with a Top Level Domain registered in IANA's Root Zone Database.

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.

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.

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

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 SecureTrust and connected to its Repository for processing 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 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 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.

Random Value: A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.

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.

Reliable Method of Communication: A method of communication, such as a postal/courier delivery address, telephone number, or email address, that was verified using a source other than the Applicant Representative.

Relying Party: Any person (Individual or entity) that relies on a Valid Certificate. An Application Software Supplier 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 Certificate status information, either in the form of a CRL or an OCSP response.

Risk Assessments: Activities defined within the SecureTrust 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 SecureTrust has in place to control such risks.

Root CA: The top level Certification Authority that issues the self-signed Root Certificate under which SecureTrust 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 SecureTrust 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 subject:organizationName 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 Identity Information: Information that identifies the Certificate Subject. Subject Identity Information does not include a domain name listed in the subjectAltName extension or the Subject commonName field.

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 CA and the Applicant/Subscriber 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.

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.

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 the EV Guidelines.

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

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

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

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

WHOIS: Information retrieved directly from the Domain Name Registrar or registry operator via the protocol defined in RFC 3912, the Registry Data Access Protocol defined in RFC 7482, or an HTTPS website.

1.6.2 Acronyms

Acronym	Meaning
ADN	Authorization Domain Name
BIS	(US Government) Bureau of Industry and Security
CA	Certification Authority
ccTLD	Country Code Top-Level Domain
CP	Certificate Policy
CPA	Chartered Professional Accountant
CPS	Certification Practices Statement
CRL	Certificate Revocation List
DBA	Doing Business As (also known as “Trading As”)
EE	End-Entity
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
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)
SPH	SecureTrust Public-Key Hierarchy
SSL	Secure Sockets Layer

Acronym	Meaning
TLD	Top-Level Domain
TLS	Transport Layer Security
TW	Trustwave
UTC(k)	National realization of Coordinated Universal Time

1.6.3 References

1. 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.
2. RFC2119 Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
3. RFC2527 Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
4. RFC2560 Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP, M. Myers, et al, June 1999.
5. RFC3279 Request for Comments: 3279, Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Polk et all, April 2002.
6. RFC3546 Request for Comments: 3546, Transport Layer Security (TLS) Extensions, Blake-Wilson et al, June 2003.
7. RFC3647 Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani et al, November 2003.
8. RFC3739 Request for Comments: 3739, Internet X.509 Public Key Infrastructure: Qualified Certificates Profile, Santesson et al, March 2004.
9. RFC4055 Request for Comments: 4055, Additional Algorithms and Identifiers for RSA Cryptography for use in the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Schaad et al, June 2005.
10. RFC5019 Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
11. RFC5280 Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
12. WebTrust for Certification Authorities – Extended Validation audit criteria, CPA Canada, 2009.
13. 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.
14. Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates https://cabforum.org/baseline-requirements-documents/
15. Guidelines for the Issuance and Management of Extended Validation Certificates https://cabforum.org/extended-validation/
16. RFC3161 Request for Comments: 3161, Internet X.509 Public Key Infrastructure: Time-Stamp Protocol (TSP), Adams et al, August 2001.
17. Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates https://aka.ms/csbr
18. NIST SP 800-56A Revision 2 NIST Special Publication 800-56A Revision 2, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, Barker et al, May 2013.

1.6.4 Conventions

The SecureTrust 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 SecureTrust.

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

SecureTrust shall maintain three separate Repositories:

1. **Certificate Repository**. SecureTrust shall make available the Root Certificates at https://certs.securetrust.com/CA. Digital Certificates that are issued to End-Entities are stored on non-public file systems and in internal databases. They may also be published to public Certificate Transparency logs in accordance with section 4.4.2 below.
2. **Document Repository**. This Certificate Policy and Certification Practice Statement, Legal documents, associated CPs, Subscriber Agreements, Relying Party Agreements, and other documents related to SecureTrust's actions as a Certificate Services Provider shall be made publicly available on our web site at the following URL: https://certs.securetrust.com/CA.
3. **Certificate Status Information Repository**. Certificate status information is available through 1) publicly published Certificate Revocation List ("CRL"). Root CRLs available at https://certs.securetrust.com/CA and/or 2) other online Certificate status protocols such as OCSP. Every Certificate issued by any CA within the SPH and governed by this CP/CPS will contain information within the Certificate that will identify the location where Certificate status information can be found. SecureTrust shall issue CRLs for all SecureTrust Certificate types, including subordinate Certification Authorities, according to the schedule defined in section 4.9.7 below.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

SecureTrust 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://certs.securetrust.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.

SecureTrust shall host test Web sites that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each root CA. These sites are accessible at the following URLs:

SGCA Valid: https://sgcatest.trustwave.com

SGCA Expired: https://sgcatest-expired.trustwave.com

SGCA Revoked: https://sgcatest-revoked.trustwave.com

STCA Valid: https://stcatest.trustwave.com

STCA Expired: https://stcatest-expired.trustwave.com

STCA Revoked: https://stcatest-revoked.trustwave.com

XGCA Valid: https://xgcatest.trustwave.com

XGCA Expired: https://xgcatest-expired.trustwave.com

XGCA Revoked: https://xgcatest-revoked.trustwave.com

TWGCA Valid: https://twgcatest.trustwave.com

TWGCA Expired: https://twgcatest-expired.trustwave.com

TWGCA Revoked: https://twgcatest-revoked.trustwave.com

TWGP256CA Valid: https://twgp256catest.trustwave.com

TWGP256CA Expired: https://twgp256catest-expired.trustwave.com

TWGP256CA Revoked: https://twgp256catest-revoked.trustwave.com

TWGP384CA Valid: https://twgp384catest.trustwave.com

TWGP384CA Expired: https://twgp384catest-expired.trustwave.com

TWGP384CA Revoked: https://twgp384catest-revoked.trustwave.com

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 1.5.4 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 according to the schedule defined in section 4.9.7.

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 SecureTrust staff. SecureTrust 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

SecureTrust 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 SecureTrust Certification Authorities shall comply with the ISO/ITU X.500 naming convention and encoded in accordance with RFC 5280.

SecureTrust does not issue Certificates that contain Internal Names.

3.1.1 Types of Names

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

3.1.1.1 EV Certificate

See EV Guidelines Section 9.2

3.1.1.2 OV SSL Certificate

In addition to the fully authenticated FQDN of the server, the subject in these Certificates shall include the following authenticated attributes:

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 SecureTrust as provided herein.
2. Locality (OID 2.5.4.7) and/or State or Province name (OID 2.5.4.8) containing Subject's address of existence or operation.
3. Country (OID 2.5.4.6) containing the two-letter ISO 3166-1 country code for the Subject's address of existence or operation.
4. Subject Alternative Name extension (OID 2.5.29.17) 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).
5. Common Name (OID 2.5.4.3) containing one of the Domain Name(s) included in the Subject Alternative Name extension.
6. Wildcard certificates are allowed.

3.1.1.3 DV Certificate

In addition to the fully authenticated FQDN of the server, the subject in these Certificates shall include the following authenticated attributes:

1. Subject Alternative Name extension (OID 2.5.29.17) 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).
2. Common name (OID 2.5.4.3) containing one of the Domain Name(s) included in the Subject Alternative Name extension.

3.1.1.4 S/MIME Certificate

The common name (OID 2.5.4.3), email address (OID 1.2.840.113549.1.9.1), and Subject Alternative Name extension (OID 2.5.29.17) shall be set to the Subscriber's email address.

3.1.1.5 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 subject in these Certificates shall include the following authenticated attributes:

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 SecureTrust as provided herein.

2. Locality (OID 2.5.4.7) and/or State or Province name (OID 2.5.4.8) containing the Subject's address of existence or operation.
3. Country (OID 2.5.4.6) containing the two-letter ISO 3166-1 country code for the Subject's address of existence or operation.

3.1.1.6 Client Authentication Certificate (client)

In addition to the sponsor-authenticated name of the Individual or device, the subject in client authentication Certificates shall include the following attributes:

1. Organization name (OID 2.5.4.10)

3.1.1.7 Timestamp Certificate

The commonName (CN) component of the subject name in Timestamp Certificates shall incorporate either "Trustwave" or "SecureTrust", "Timestamping Responder", and a unique identifier such as the year of Certificate/Private Key generation. In addition, the subject in these Certificates shall include the following authenticated attributes:

1. Organization name (OID 2.5.4.10) containing Trustwave's full legal organization name as listed in the official records of the Incorporating or Registration Agency in Trustwave's Jurisdiction of Incorporation or Registration.
2. Locality (OID 2.5.4.7) and State or Province name (OID 2.5.4.8) containing Trustwave's address of existence or operation.
3. Country (OID 2.5.4.6) containing the two-letter ISO 3166-1 country code for Trustwave's address of existence or operation.

3.1.2 Need for Names to be Meaningful

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

Certificate Type	*Description of the Need for the Name to be Meaningful*
1. EV Certificate	SecureTrust ensures via the practices and procedures defined within this document, specifically in section 3.2.2, that the subject name uniquely identifies the name of the Subscriber.
2. OV SSL Certificate	SecureTrust ensures via the practices and procedures defined within this document, specifically in section 3.2.2, that the subject name uniquely identifies the name of the Subscriber.
3. OV Code Signing Certificate	SecureTrust ensures via the practices and procedures defined within this document, specifically in section 3.2.2, that the subject name uniquely identifies the name of the Subscriber.
4. DV Certificate	SecureTrust ensures via the practices and procedures defined within this document, specifically in section 3.2.2, that the subject name uniquely identifies the name of the Subscriber.
5. Timestamp Certificate	SecureTrust ensures via the practices and procedures defined within this document, specifically in section 3.2.2, that the subject name uniquely identifies the name of the Subscriber.
6. Client Authentication Certificate	The Sponsor is responsible for subject names.
7. S/MIME Certificate	The Sponsor is responsible for subject names.

Table 4

3.1.3 Anonymity or Pseudonymity of Subscribers

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

3.1.4 Rules for Interpreting Various Name Forms

Name forms within SecureTrust Certification Authority Certificates, SecureTrust-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 SecureTrust issued Certificates shall be determined as set forth below:

Certificate Type	*Uniqueness of Name Requirement*
1. EV Certificate	The subject of all Certificates issued by SecureTrust shall be unique.
2. OV SSL Certificate	The subject of all Certificates issued by SecureTrust shall be unique.
3. DV certificate	The subject of all Certificates issued by SecureTrust shall be unique.
4. OV Code Signing Certificate	The subject of all Certificates issued by SecureTrust shall be unique.
5. Client Authentication Certificate	The subject of all Certificates issued by SecureTrust shall be unique.
6. Timestamp Certificate	The subject of all Certificates issued by SecureTrust shall be unique.
7. S/MIME Certificate	The subject information in a S/MIME Certificate is limited to an authenticated email address. While typically a unique email address would correspond to a unique individual, there are no guarantees as to the uniqueness of the individuals with access to that email address.

Table 5

3.1.6 Recognition, Authentication, and Role of Trademarks

SecureTrust 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. SecureTrust 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

Prior to the use of an Incorporating Agency or Registration Agency to validate organization identity for Applicants of EV Certificates, the Incorporating Agency or Registration Agency must be disclosed in SecureTrust’s Repository at https://certs.securetrust.com/CA/registry-list.php.

3.2.1 Method to Prove Possession of Private Key

All End-Entity applicants for all certificate types within the SPH 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. SecureTrust 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

For OV SSL Certificates, EV Certificates, and OV Code Signing Certificates, SecureTrust shall verify the identity of the Applicant and the authenticity of the Applicant Representative’s certificate request using a verification process meeting the requirements of Section 3.2.2.1. SecureTrust shall inspect any document relied upon under this Section for alteration or falsification.

3.2.2.1 Identity

1. EV Certificates require extensive identity verification as defined in the CABF EV Guidelines located here: https://cabforum.org/extended-validation/

2. OV SSL and OV Code Signing Certificates include the name and location fields of the organization. These are verified using documentation or communication with one or more of the following:
    a. A governmental agency in the jurisdiction of the Applicant's legal creation, existence, or recognition. Communication may include look-up on a database such as a Secretary of State website or documents such as Articles of Incorporation, Certificate of Incorporation, L.L.C., L.L.P., L.P., L.T.D., Fictitious Name, or any other standard documentation issued by or filed with the proper governmental authority.
    b. A third party data source meeting the requirements in Section 3.2.2.7
    c. An Attestation letter.
    d. For location only, a utility bill, bank statement, credit card statement, or government issued tax document.

3.2.2.2 DBA/Tradename

1. EV Certificates require extensive identity verification as defined in the CABF EV Guidelines section 11.3.
2. OV SSL and OV Code Signing Certificates include the name and location fields of the organization. These are verified using documentation or a Reliable Method of Communication with the following:
    a. A governmental agency in the jurisdiction of the Applicant's legal creation, existence, or recognition. Communication may include look-up on a database such as a Secretary of State website or documents such as Articles of Incorporation, Certificate of Incorporation, L.L.C., L.L.P., L.P., L.T.D., Fictitious Name, DBA, or any other standard documentation issued by or filed with the proper governmental authority.
    b. A third party data source meeting the requirements in Section 3.2.2.7
    c. An Attestation letter accompanied by documentary support.
    d. A utility bill, bank statement, credit card statement, or government issued tax document. (Note that in Section 3.2.2.1 these can only be used for location, but here they can also be used for DBA/ Tradename.)

3.2.2.3 Verification of Country

Any method in Section 3.2.2.1 shall be used to verify country.

3.2.2.4 Authorization by Domain Name Registrant

All the following methods apply to all DV, OV SSL, and EV SSL certificates unless otherwise stated.

As of the date the Certificate issues, SecureTrust shall validate each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated no more than 825 days (DV/OV SSL) or 13 months (EV) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact directly with the Domain Name Registrar by using a WHOIS lookup.

This method was deprecated by the CA/Browser Forum. SecureTrust no longer uses this method.

3.2.2.4.2 Email Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address identified as a Domain Contact.

Each email may confirm control of multiple Authorization Domain Names.

SecureTrust may send the email identified under this section to more than one recipient provided that every recipient is identified by the Domain Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email.

The Random Value SHALL be unique in each email.

SecureTrust may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

Confirming the Applicant's control over the requested FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. SecureTrust must place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.

This method was deprecated by the CA/Browser Forum. SecureTrust no longer uses this method.

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the requested FQDN by (i) sending an email to one or more addresses created by using 'admin', 'administrator', 'webmaster', 'hostmaster', or 'postmaster' as the local part, followed by the at-sign ("@"), followed by an Authorization Domain Name, (ii) including a Random Value in the email, and (iii) receiving a confirming response utilizing the Random Value.

Each email may confirm control of multiple FQDNs, provided the Authorization Domain Name used in the email is an Authorization Domain Name for each FQDN being confirmed.

The Random Value shall be unique in each email.

The email may be re-sent in its entirety, including the re-use of the Random Value, provided that its entire contents and recipients shall remain unchanged.

The Random Value shall remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.5 Domain Authorization Document

SecureTrust does not utilize this method of validation.

3.2.2.4.6 Agreed-Upon Change to a Website

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value (contained in the content of a file) under the "/.well-known/pki-validation" directory, or another path registered with IANA for the purpose of Domain Validation, on the Authorization Domain Name that is accessible to SecureTrust via HTTP/HTTPS over an Authorized Port.

SecureTrust shall provide a Random Value unique to the certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of the CA/Browser Forum Baseline Requirements or Section 11.14.3 of the CA/Browser Forum EV SSL Certificate Guidelines). The Random Value shall not be included in the request used by SecureTrust to confirm the presence of the Random Value.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

SecureTrust SHALL NOT perform validation using this method after May 31, 2020. SecureTrust MAY continue to re-use information and validations for domains validated under this method per the applicable certificate data reuse periods.

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value in a DNS TXT or CAA record for either 1) an Authorization Domain Name; or 2) an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

SecureTrust shall provide a Random Value unique to the certificate request and shall not use the Random Value after (i) 30 days or (ii) if the Applicant submitted the certificate request, the timeframe permitted for reuse of validated information relevant to the certificate (such as in Section 4.2.1 of the CA/Browser Forum Baseline Requirements or Section 11.14.3 of the CA/Browser Forum EV SSL Certificate Guidelines).

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.8 IP Address

SecureTrust does not utilize this method of validation.

3.2.2.4.9 Test Certificate

SecureTrust does not utilize this method of validation.

3.2.2.4.10 TLS Using a Random Number

SecureTrust does not utilize this method of validation.

3.2.2.4.11 Any Other Method

SecureTrust does not utilize this method of validation.

3.2.2.4.12 Validating Applicant as a Domain Contact

SecureTrust does not utilize this method of validation.

3.2.2.4.13 Email to DNS CAA Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set MUST be found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065 (Appendix A).

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS CAA Email Contact for each Authorization Domain Name being validated.

SecureTrust may send the email identified under this section to more than one recipient provided that every recipient is a DNS CAA Email Contact for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email.

SecureTrust may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.14 Email to DNS TXT Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to a DNS TXT Record Email Contact.

Each email may confirm control of multiple FQDNs, provided that each email address is a DNS TXT Record Email Contact for each Authorization Domain Name being validated.

SecureTrust may send the email identified under this section to more than one recipient provided that every recipient is a DNS TXT Record Email Contact for each Authorization Domain Name being validated.

The Random Value SHALL be unique in each email.

SecureTrust may resend the email in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.15 Phone Contact with Domain Contact

Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and a confirming response is provided for each ADN.

In the event that someone other than a Domain Contact is reached, SecureTrust MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, SecureTrust MAY generate and leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to SecureTrust to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same DNS TXT Record Phone Contact phone number is listed for each ADN being verified and a confirming response is provided for each ADN.

SecureTrust SHALL NOT request to be transferred, as this phone number is specifically listed for the purpose of Domain Validation. A response using this method SHALL NOT be considered valid if SecureTrust is knowingly transferred.

In the event of reaching voicemail, SecureTrust MAY generate and leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to SecureTrust to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust may also issue certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

SecureTrust does not utilize this method of validation.

3.2.2.4.18 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file.

1. The entire Request Token or Random Value SHALL NOT appear in the request used to retrieve the file, and
2. SecureTrust MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file containing the Request Token or Random Number:

1. MUST be located on the Authorization Domain Name, and
2. MUST be located under the "/.well-known/pki-validation" directory, and
3. SHALL be retrieved via either the "http" or "https" scheme, and
4. SHALL be accessed over an Authorized Port.

If SecureTrust follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.
2. Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3.
3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
4. Redirects MUST be to resource URLs with either the “http” or “https” scheme.
5. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. SecureTrust SHALL provide a Random Value unique to the certificate request.
2. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Note: Once the FQDN has been validated using this method, SecureTrust MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

Confirming the Applicant’s control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555. The following are additive requirements to RFC 8555.

SecureTrust MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The token (as defined in RFC 8555, section 8.3) SHALL NOT be used for more than 30 days from its creation.

If SecureTrust follows redirects, the following apply:

1. Redirects MUST be initiated at the HTTP protocol layer.
2. Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3.
3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
4. Redirects MUST be to resource URLs with either the “http” or “https” scheme.
5. Redirects MUST be to resource URLs accessed via Authorized Ports.

Note: Once the FQDN has been validated using this method, SecureTrust MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.5 Authentication for an IP Address

SecureTrust does not issue certificates containing IP addresses.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, SecureTrust follows an automated procedure that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix” (e.g. “*.com”, “*.co.uk”, see RFC 6454 Section 8.2 for further explanation). SecureTrust relies upon periodically updated data from https://publicsuffix.org for identifying which components of a given name are “registry-controlled”.

3.2.2.7 Data Source Accuracy

SecureTrust maintains a list of accepted data sources that consider the following:

1. The age of the information provided,
2. The frequency of updates to the information source,
3. The data provider and purpose of the data collection,
4. The public accessibility of the data availability, and

5. The relative difficulty in falsifying or altering the data.

3.2.2.8 CAA Records

As part of the issuance process, SecureTrust checks for relevant Certification Authority Authorization (CAA) DNS records for each dNSName in the subjectAltName extension of Certificates to be issued as specified in RFC 6844 and amended by IETF Erratum 5065.

SecureTrust recognizes either “trustwave.com” or “securetrust.com” as an identifying Domain Name for “issue” and “issuewild” CAA records.

3.2.3 Authentication of Individual Identity

3.2.3.1 EV Certificates

EV certificates shall not be issued to individuals.

3.2.3.2 OV SSL and OV Code Signing Certificates

If the Subject is a natural person, then SecureTrust shall verify the Applicant’s name, Applicant’s address, and the authenticity of the certificate request.

1. SecureTrust shall verify the Applicant’s name using a legible copy, which discernibly shows the Applicant’s face, of at least one currently valid government-issued photo ID (passport, driver’s license, military ID, national ID, or equivalent document type). SecureTrust shall inspect the copy for any indication of alteration or falsification.
2. SecureTrust shall verify the Applicant’s address using a form of identification deemed to be reliable, such as a government ID, utility bill, or bank or credit card statement. This includes the same government-issued ID that was used to verify the Applicant’s name.
3. SecureTrust shall verify the certificate request with the Applicant using a Reliable Method of Communication.

3.2.3.3 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 SecureTrust proprietary data, including without limitation all non-public information regarding the SPH, in strict confidence.

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

1. Sponsor shall receive one official identification document as issued by governmental authorities having the jurisdiction to issue such documents.
2. At least one document shall contain a picture of the current likeness of the Individual Applicant.
3. Any one of these documents must always be presented:
    a. Driver’s license or identification card as issued by the state or locale of the Applicant’s legal residence;
    b. U.S. Passport;
    c. Certified birth certificate issued by the city, county, or state of birth, in accordance with applicable law;
    d. 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;
    e. Certificate of Citizenship issued by USCIS;
    f. Department of State Form FS-240 – Consular Report of Birth; or
    g. Department of State Form DS-1350 – Certification of Report of Birth.
4. 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.

3.2.3.4 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 SecureTrust, nor shall it be contained within the final Certificate issued by SecureTrust. SecureTrust will confirm that

the Applicant holds the private key corresponding to the public key to be included in the Certificate. SecureTrust performs a limited confirmation of the Certificate Applicant's email address through the following request-response mechanism:

1. SecureTrust receives a request for an S/MIME Certificate.
2. SecureTrust 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.
3. The Applicant shall click on the link which will take them to a webpage.
4. The Applicant then confirms their information and clicks a button asking for the Certificate to be issued.
5. An RSA key pair is generated on the Applicant's computer.
6. A certificate request containing the public key from the generated key pair is sent from the Applicant's computer to SecureTrust.
7. The Certificate is then issued and provided to the Subscriber in the form of a download link.

3.2.4 Non-Verified Subscriber Information

All information contained within Certificates issued by SecureTrust will be verified, except as it may have otherwise been stated in section 3.1.1 for S/MIME Certificates and/or Client Authentication Certificates.

3.2.5 Validation of Authority

Certificate Type	*Description*
1. EV Certificate	**See EV Guidelines Section 11.8 and 11.11 (https://cabforum.org/extended-validation/)**
2. OV SSL Certificate, OV Code Signing Certificate, Client Authentication Certificate, Timestamp Certificate	See Section 3.2.2

Table 6

3.2.6 Criteria for Interoperation

SecureTrust shall publicly disclose all Cross Certificates in the Common CA Database (CCADB) within seven days of creation.

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 Certificate Re-key. Subscribers shall generate a new Key Pair to replace the expiring Key Pair. Identification and authentication of the request will be performed in accordance with the procedures in Section 3.2.

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

SecureTrust shall authenticate Certificate revocation requests to confirm that such requests are from the Subscriber.

For manual requests, and as per section 4.9.2, the request must come from an appropriate Subscriber-designated representative. SecureTrust will communicate via email or phone number on file to the Subscriber's administrative or technical contacts and must receive confirmation of the revocation request.

For automated requests, a Subscriber-designated contact must login to their SecureTrust accounts with username and password to request the revocation and another Subscriber-designated contact must separately login with username and password to approve the revocation.

The process for revocation is further explained in section 4.9.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

This CP/CPS defines operational policies and the requirements of our Certification Authority that pertain to all types of Certificates issued by SecureTrust.

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.

4.1.1.1 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.

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

1. **Private Organization Subjects**

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

   a. 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;
   b. 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;
   c. 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;
   d. The Private organization MUST have a verifiable physical existence and business presence;
   e. The Private Organization’s Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business MUST NOT be in any country where SecureTrust is prohibited from doing business or issuing a certificate by the laws of SecureTrust’s jurisdiction; and
   f. The Private Organization MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of SecureTrust’s jurisdiction.

2. **Government Entity Subjects**

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

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

3. **Business Entity Subjects**

   SecureTrust MAY issue EV Certificates to Business Entities who do not qualify under Section 1 but that do satisfy the following requirements:

   a. 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;
   b. The Business Entity MUST have a verifiable physical existence and business presence;
   c. At least one Principal Individual associated with the Business Entity MUST be identified and validated;
   d. The identified Principal Individual MUST attest to the representations made in the Subscriber Agreement;

e. Where the Business Entity represents itself under an assumed name, SecureTrust MUST verify the Business Entity's use of the assumed name pursuant to the requirements herein;
f. The Business Entity and the identified Principal Individual associated with the Business Entity MUST NOT be located or residing in any country where SecureTrust is prohibited from doing business or issuing a certificate by the laws of SecureTrust's jurisdiction; and
g. 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 SecureTrust's jurisdiction.

4. **Non-Commercial Entity Subjects**

   SecureTrust MAY issue EV Certificates to Non-Commercial Entities who do not qualify under Sections 1, 2 or 3, but satisfy the following requirements:

   a. 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. The CA/Browser Forum may publish a listing of International Organizations that have been approved for EV eligibility; and
   b. The International Organization Entity MUST NOT be headquartered in any country where SecureTrust is prohibited from doing business or issuing a certificate by the laws of Trustwave's jurisdiction; and
   c. The International Organization Entity MUST NOT be listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of SecureTrust's jurisdiction.

4.1.1.2 OV SSL Certificate

Applications for OV SSL Certificates shall be submitted by either 1) the administrative, registrant, or technical contact associated with the WHOIS record for the domain, or 2) SecureTrust shall verify the Certificate Approver is expressly authorized by the Applicant by one of the following:

1. A Verified Legal Opinion or Verified Accountant Letter which states that the Certificate requester has Certificate requesting authority;
2. SecureTrust can obtain a corporate resolution from the Applicant which states the Certificate requester has the Certificate requesting authority. This resolution shall be certified by the appropriate company officer, and SecureTrust shall be able to reliably verify the company officer has signed the resolution and that he/she has the authority to sign the resolution;
3. SecureTrust can obtain confirmation from the Applicant which states the Contract Signer has the signing authority and the Certificate Approver has the requesting authority; or
4. SecureTrust and Applicant may mutually enter into a contract which states that the Certificate requester has requesting authority.

4.1.1.3 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:

1. A Verified Legal Opinion or Verified Accountant Letter which states that the Certificate requester has Certificate requesting authority;
2. SecureTrust can obtain a corporate resolution from the Applicant which states the Certificate requester has the Certificate requesting authority. This resolution shall be certified by the appropriate company officer, and SecureTrust shall be able to reliably verify the company officer has signed the resolution and that he/she has the authority to sign the resolution;
3. SecureTrust can obtain confirmation from the Applicant which states the Contract Signer has the signing authority and the Certificate Approver has the requesting authority; or
4. SecureTrust and Applicant may mutually enter into a contract which states that the Certificate requester has requesting authority.

4.1.1.4 S/MIME Certificate

SecureTrust accepts applications for S/MIME Certificates from individuals or organizations who can demonstrate control over the named email address.

4.1.1.5 DV Certificate

SecureTrust accepts applications for DV Certificates from individuals or organizations who can demonstrate control over the named domain.

4.1.1.6 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.

4.1.1.7 Timestamp Certificate

SecureTrust does not accept applications for Timestamp Certificates. Timestamp Certificates are only issued to SecureTrust for internal use.

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. Alternatively, the applicant may submit a Signed Public Key and Challenge (SPKAC) for Client Authentication Certificate and S/MIME Certificate types only.

4.1.2.1 EV Certificate

The following Applicant roles are required for the issuance of an EV Certificate.

1. **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.
2. **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.
3. **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.
4. **Applicant Representative**: Terms of Use applicable to the requested EV Certificate must be acknowledged and agreed to by an authorized Applicant Representative.

One person may be authorized by Applicant to fill one or more of these roles, provided that the Certificate Approver and Contract Signer are employees of Applicant. An Applicant may also authorize more than one person to fill each of these roles. Following completion of contract arrangements as per section 3.2.5, the applicant shall submit the PKCS #10 Certificate Signing Request ("CSR") for initial application processing.

4.1.2.2 Other Certificate Types

Applicants for OV SSL Certificates, DV Certificates, OV Code Signing Certificates, S/MIME Certificates, or Client Authentication Certificates to be issued by SecureTrust shall follow the registration procedures as defined by SecureTrust. The primary steps for a Certificate registration are:

1. Valid identification documentation is provided and complete registration forms have been signed;
2. The CP/CPS and End-User Agreement have been accepted by the Subscriber; and
3. All documents and information provided by Applicant are approved by SecureTrust.

4.2 CERTIFICATE APPLICATION PROCESSING

See section 3.2.2.8 for SecureTrust's practice on processing CAA Records for Fully Qualified Domain Names.

4.2.1 Performing Identification and Authentication Functions

4.2.1.1 EV Certificate

Before issuing a Certificate, SecureTrust shall ensure that all Subject Identity 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 SecureTrust pursuant to the verification processes. The verification process shall accomplish:

1. Verification of Applicant's existence and identity, including:
    a. Verify Applicant's legal existence and identity
    b. Verify Applicant's physical existence
    c. Verify Applicant's operational existence
2. Verify Applicant is a registered holder or has exclusive control of the domain name
3. Verify Applicant's authorization for requesting the Certificate including:
    a. Verify the name, title, and authority of the contract signer, Certificate Approver, and Certificate Requester.
    b. Verify that Contract Signer signed the Subscriber Agreement, and
    c. Verify that a Certificate Approver has signed or otherwise approved the Certificate request

Maximum Validity Period for Validated Data

The age of validated data used to support issuance of a Certificate (before revalidation is required) shall not exceed the following limits:

1. Legal existence and identity – 13 months;
2. Assumed name – 13 months;
3. Address of Place of Business – 13 months, but thereafter data MAY be refreshed by checking a Qualified Independent Information Source
4. Telephone number for Place of Business – 13 months;
5. Bank account verification – 13 months;
6. Domain name – 13 months;
7. Identity and authority of Certificate Approver – 13 months, unless a contract is in place between SecureTrust and Applicant that specifies a different term, in which case, the term specified in such contract will control. For example, the contract MAY use terms that allow the assignment of roles that are perpetual until revoked, or until the contract expires or is terminated.

Note on Reuse and Updating Information and Documentation

1. Use of Documentation to Support Multiple Certificates SecureTrust 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.
2. Use of Pre-Existing Information or Documentation
    a. Each Certificate issued by SecureTrust 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.
    b. The age of information used by SecureTrust 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 SecureTrust 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).
    c. In the case of outdated information, SecureTrust shall repeat the verification processes required in this CP/CPS.

4.2.1.1 OV SSL Certificate

When a Subscriber does not have a pre-existing Certificate, prior to issuing the Subscriber its new Certificate, SecureTrust 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. SecureTrust may use any combination of validation procedures to validate this information, and organizational information may be validated at a different time than the domain name information. However, both the organizational

information and the domain name information shall be validated prior to a Certificate being issued by SecureTrust. Once both the organizational information and the domain name information are validated, the Subscriber's Certificate will be issued.

Maximum Validity Period for Validated Data

The age of validated data used to support issuance of a Certificate (before revalidation is required) shall not exceed 825 days.

4.2.1.2 OV Code Signing Certificate

When a Subscriber does not have a pre-existing Certificate, prior to issuing the Subscriber its new Certificate, SecureTrust 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. SecureTrust 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 SecureTrust. Once the organizational information is validated, the Subscriber's Certificate will be issued.

4.2.1.3 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 SecureTrust. SecureTrust will confirm that the Applicant holds the private key corresponding to the public key to be included in the Certificate. SecureTrust also performs a limited confirmation of the Certificate Applicant's email address following the request/response mechanism in Section 3.2.3.2.

4.2.1.4 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. Acceptable means of correlation by the applicable Sponsor may include the following:

- A designated representative from the Applicant's company, or a Trustwave employee, shall be responsible for collecting the two components of identity evidence (see Section 3.2.3.3) associated with the Applicant.
- The designated representative from the Applicant's company, or a Trustwave employee, shall verify that the photograph from the representative documentation collected in Section 3.2.3.3 is a reasonable likeness of the Applicant.
- 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.
- SecureTrust shall attribute the password provided to the Applicant to a profile stored on SecureTrust enrollment servers.
- The Applicant shall connect to SecureTrust'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 email address for notification upon completion of the Certificate generation by SecureTrust. Furthermore, the Applicant will be provided with a single use pass code, necessary for collection of the client authentication Certificate upon issuance by SecureTrust. Using the pass code provided within the browser in the previous step, the Applicant shall connect to the SecureTrust enrollment servers to receive the final Certificate.

4.2.1.5 DV certificate

See Section 4.1.2

Maximum Validity Period for Validated Data

The age of validated data used to support issuance of a Certificate (before revalidation is required) shall not exceed 825 days.

4.2.1.6 High Risk Status (applicable to EV, DV, OV SSL and OV Code Signing certificates only)

1. Verification Requirements.

SecureTrust takes reasonable measures to identify high risk certificate requests likely to be targeted for fraudulent attacks (“High Risk Certificate Request”). SecureTrust conducts additional verification and takes reasonable precautions necessary to ensure that such certificate requests are properly verified in accordance with the CA/Browser Forum Guidelines.

2. Acceptable Methods of Verification.

   SecureTrust may identify High Risk Certificate Requests 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. DV, OV SSL, and OV Code Signing certificates may be identified as High Risk in a similar manner. Examples of such lists include: Anti-Phishing Work Group list of phishing targets and internal SecureTrust 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 a certificate request is flagged as a High Risk Certificate Request, SecureTrust 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. Denied Lists and Other Legal Black Lists (applicable to EV certificates only)

4. Verification Requirements

   SecureTrust 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.

   SecureTrust 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.

5. Acceptable Methods of Verification

   SecureTrust 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

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 Section 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:

1. EV Certificates – 10 business days
2. All other certificate types - 2 business days

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Following successful completion of all relevant sections within Section 3.1 and Section 4.2, SecureTrust, 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 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, SecureTrust may include a Latin character organization name in an OV SSL or EV certificate. In such a case, SecureTrust shall comply with the following process.

In order to include a transliteration/Romanization of the registered name, the Romanization shall be verified by SecureTrust using a system officially recognized by the Government in the Applicant's jurisdiction of incorporation. If SecureTrust 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 SecureTrust shall rely on one of the options below, in order of preference:

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

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

SecureTrust shall notify the Applicant that the Certificate has been issued via either email, 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 email.

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

SecureTrust publishes all DV, OV SSL, and EV End-Entity Certificates it issues in public Certificate Transparency log servers in accordance with Google Chrome Certificate Transparency Policy and Apple Certificate Transparency Policy. SecureTrust does not publish other types of Certificates to public Certificate Transparency log servers.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

SecureTrust may notify RAs, partners, or resellers of the Certificate issuance if they were involved in the initial enrollment.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers, for all forms of SecureTrust-issued Certificates, shall

1. Possess at least a rudimentary knowledge of public key cryptography and Certificates;
2. Have completed all necessary enrollment forms and have executed payment for all accounts due;
3. Read and agree to this CP/CPS, any and all relevant CPs, and any and all Subscriber Agreements;
4. Protect their private key from unauthorized access and Compromise;
5. Not share their private key and/or passwords protecting their private key;
6. Notify SecureTrust of any change to the information contained within the Certificate;
7. Comply with all laws and regulations applicable to the export, import, and use of Certificates issued by SecureTrust; and
8. Except as otherwise set forth herein, in no event, use a Certificate issued by SecureTrust for the purpose of signing a document with the intent to authenticate and create a legally binding signature.

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

Certificate Type	*Private key and certificate usage*
EV Certificate, OV SSL, DV Certificate	These Certificates shall serve only to authenticate a server to a client.
S/MIME Certificate	These Certificates shall only be used to facilitate an S/MIME transaction between two email 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 authentication for VPN tunnel endpoints.
Timestamp Certificate	These Certificates shall only be used to provide Trusted Timestamp services.

Table 7

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall:

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

Relying parties shall not:

1. Rely on a digital signature within the SPH 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.

4.6.1 Circumstance for Certificate Renewal

An existing Subscriber may request renewal of a certificate that is either nearing expiration or recently expired, as long as the information in the previous certificate is still accurate. The Subscriber shall pay the fees and comply with the other terms and conditions for renewal.

4.6.2 Who May Request Renewal

The Subscriber or an authorized representative of the Subscriber may request renewal. SecureTrust may initiate a certificate renewal in the event that the issuing CA is re-keyed.

4.6.3 Processing Certificate Renewal Requests

For purposes of this CP/CPS, and for all Certificates issued within the SPH, 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 SecureTrust upon issuance of the renewal Certificate.

4.6.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

See Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

See Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Certificate re-key involves a process whereby a Subscriber with an existing valid certificate generates a new key pair and applies for the issuance of a replacement certificate that certifies the new key pair.

4.7.1 Circumstance for Certificate Re-key

Prior to the expiration of an existing Subscriber's Certificate, a Subscriber may need or choose to re-key their certificate as part of a hardware or software change or other reasons at their discretion.

4.7.2 Who May Request Certification of a New Public Key

The Subscriber or an authorized representative of the Subscriber may request certificate re-key.

4.7.3 Processing Certificate Re-keying Requests

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 SecureTrust upon issuance of the new Certificate.

4.7.4 Notification of New Certificate Issuance to Subscriber

See Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate

See Section 4.4.1.

4.7.6 Publication of the Re-keyed Certificate by the CA

See Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Certificate modification is the process through which a Subscriber requests a Certificate with modified subject information. SecureTrust 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

Not applicable.

4.8.2 Who May Request Certificate Modification

Not applicable.

4.8.3 Processing Certificate Modification Requests

Not applicable.

4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

4.8.6 Publication of the Modified Certificate by the CA

Not applicable.

4.8.7 Notification of Certificate Issuance by the CA to Other Entities

Not applicable.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

4.9.1 Circumstances for Revocation

Certificate revocation is the process by which SecureTrust prematurely terminates the Validity Period of a Certificate by posting the serial number of the Certificate to a Certificate Revocation List.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

SecureTrust will revoke the Certificate within 24 hours when any of the following events occurs:

1. The Subscriber requests, in writing, revocation of its Certificate;
2. The Subscriber indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. SecureTrust obtains reasonable evidence that the Subscriber's Private Key (corresponding to the Public Key in the Certificate) has been Compromised; or
4. SecureTrust obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name or IP address in the Certificate should not be relied upon.

SecureTrust will revoke the Certificate within 5 days if one or more of the following events occur:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. SecureTrust obtains evidence that the Certificate has otherwise been misused;
3. SecureTrust receives notice or otherwise becomes aware that a Subscriber violates any of its material obligations under the Subscriber Agreement;
4. SecureTrust 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;
5. SecureTrust is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. SecureTrust receives notice or otherwise becomes aware of a material change in the information contained in the Certificate;
7. A determination, in SecureTrust's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the applicable CP;
8. SecureTrust determines that any of the information appearing in the Certificate is not accurate;
9. SecureTrust ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
10. SecureTrust's right to issue Certificates under these Requirements expires or is revoked or terminated, unless SecureTrust has made arrangements to continue maintaining the CRL/OCSP Repository;
11. SecureTrust's Private Key for that Certificate has been compromised;
12. Such additional revocation events as SecureTrust publishes;
13. Upon approval by the CPB;
14. SecureTrust 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 SecureTrust's jurisdiction of operation;
15. The Subscriber intentionally includes Suspect Code in its signed software; or
16. SecureTrust 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.
17. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/ signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by SecureTrust within a given period of time).
18. SecureTrust receives notice or otherwise becomes aware of any circumstance indicating that use of the email address in the Certificate is no longer legally permitted.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

SecureTrust will revoke the Certificate within seven (7) days when any of the following events occurs:

1. The Subordinate CA requests, in writing, revocation of its Certificate;
2. The Subordinate CA indicates that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. SecureTrust obtains reasonable evidence that the Subordinate CA's Private Key (corresponding to the Public Key in the Certificate) has been Compromised or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. A determination, in SecureTrust's sole discretion, that the Certificate was not issued in accordance with the terms and conditions of this CP/CPS or the applicable CP;
5. A determination, in SecureTrust's sole discretion, that the Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. SecureTrust determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. SecureTrust or the Subordinate CA ceases operations for any reason and has not arranged for another CA to provide revocation support for the Certificate;
8. SecureTrust's or the Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless SecureTrust has made arrangements to continue maintaining the CRL/OCSP Repository;
9. Such additional revocation events as SecureTrust publishes;
10. Upon approval by the CPB;
11. SecureTrust 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 SecureTrust's jurisdiction of operation;
12. SecureTrust 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.
13. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/ signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by SecureTrust within a given period of time).

4.9.2 Who Can Request Revocation

The Subscriber (including designated representatives; Certificate Approver, Contract Signer) can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing SecureTrust of reasonable cause to revoke the certificate.

SecureTrust reserves the right to unilaterally revoke any certificate issued within the SPH without cause.

4.9.3 Procedure for Revocation Request

To request revocation, a Subscriber shall contact SecureTrust, either by email message to cert-problem-report@securetrust.com, 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, SecureTrust will seek confirmation of the request by email message to the person requesting revocation (as defined in Section 4.9.2 above). The message will state that, upon confirmation of the revocation request, SecureTrust 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. SecureTrust shall require a confirming email message back from either the administrative or technical contact authorizing revocation (or by other means of confirmation acceptable to SecureTrust). Upon receipt of the confirming email message, SecureTrust 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 SecureTrust 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 SecureTrust's Private Key used to sign a Certificate, SecureTrust shall send an

email 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.

Subscribers may request revocation for a Certificate by using the revocation functionality in the SecureTrust portal or by using the revocation functionality in automated Certificate lifetime management protocols supported by SecureTrust.

1. In the SecureTrust portal, SecureTrust will work with the Subscriber to assign at least two users the ability to revoke Certificates. When enabled, Certificates will have a “revoke” button associated with them. Once approved, the user must click the “revoke” button which will send emails to the other approved users with instructions for approving the revocation request. When the second approved user clicks the “revoke” button, the Certificate shall be revoked.
2. For the automated Certificate lifetime management protocols supported by SecureTrust, the revocation procedure is outlined in the specification for the protocol.

For the methods outlined above, Subscribers may optionally specify a revocation reason code to inform Relying Parties of the reason for the Certificate revocation. SecureTrust does not validate that Subscriber-supplied reason codes are appropriate irrespective of the facts and circumstances surrounding the revocation request.

Relying Parties, Application Software Suppliers, and other third parties shall contact SecureTrust by email message (See email address in section 1.5.2) to report suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates.

4.9.4 Revocation Request Grace Period

See Section 4.9.3

4.9.5 Time within Which CA Must Process the Revocation Request

See Section 4.9.3 for a Subscriber-initiated revocation.

For a Certificate Problem Report, SecureTrust will begin investigation within twenty-four hours of receipt and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

Within the timelines defined in Section 4.9.1.1, SecureTrust will make a determination whether revocation is required and revoke the Certificate(s) in question. In selecting the revocation date within the timelines defined in Section 4.9.1.1, SecureTrust will consider the following criteria:

1. The nature of the alleged problem;
2. The consequences of revocation;
3. The number of Certificate Problem Reports received on a particular Certificate or Subscriber;
4. The entity making the complaint;
5. Relevant legislation.

4.9.6 Revocation Checking Requirement for Relying Parties

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

4.9.7 CRL Issuance Frequency

All certification authorities within the SPH that have issued any End-Entity Certificates shall issue CRLs on at least a daily basis. Other certification authorities within the SPH shall issue CRLs at least annually.

4.9.8 Maximum Latency for CRLs

The maximum latency for any CRL issued by a certificate authority within the SPH that has issued any End-Entity Certificates shall be twelve hours from its time of issuance until its availablility in the repository. The maximum latency for other certificate authorities shall be one day from its time of issuance until its availability in the repository.

4.9.9 On-line Revocation/Status Checking Availability

Issuance and revocation status checking services are available at http://ocsp.securetrust.com for certificates issued from any of the certification authorities within the SPH. Responses conform to RFC 5019 and/or RFC 6960, and may be signed by the CA that issued the certificate, by a delegated OCSP responder certificate containing the id-pkix-ocsp-nocheck extension and issued by the CA that issued the certificate, or may be unsigned in the case of an unknown certificate, in accordance with RFC 5019 section 2.2.3.

Accurate OCSP responses are available immediately upon certificate issuance or revocation.

4.9.10 On-line Revocation Checking Requirements

SecureTrust supports an OCSP capability using the GET method. The OCSP responder will not respond with a “good” status if the certificate has not been issued. OCSP responses have a validity period of no more than 5 days, and a newer response is available before ½ of the validity period has expired.

4.9.11 Other Forms of Revocation Advertisements Available

SecureTrust allows its subscribers to use OCSP stapling, but does not require them to do so.

4.9.12 Special Requirements Re Key Compromise

Reports of key compromise to SecureTrust MUST include proof of key compromise in one of the following formats:

- A CSR with the Common Name “Proof of Key Compromise for SecureTrust”, signed by the compromised private key, or
- The compromised private key itself.

4.9.13 Circumstances for Suspension

No certification authority within the SPH shall suspend Certificates.

4.9.14 Who Can Request Suspension

See section 4.9.13.

4.9.15 Procedure for Suspension Request

See section 4.9.13.

4.9.16 Limits on Suspension Period

See section 4.9.13.

4.10 CERTIFICATE STATUS SERVICES

4.10.1 Operational Characteristics

CRL access for SecureTrust root certificates is located at the following URL:

https://certs.securetrust.com/CA

URLs for checking validity of intermediate CA and end entity certificates using OCSP or CRL are provided in the certificate itself, in the Certificate Authority Information Access and CRL distribution Points extensions, respectively.

Revocation entries will not be removed until after the expiry date of the revoked certificate. In the case of revoked code signing certificates, entries will not be removed until at least ten (10) years following the expiry date of the revoked certificate.

4.10.2 Service Availability

SecureTrust 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.

SecureTrust's CRL and OCSP capabilities shall be maintained with resources sufficient to provide a response time of less than ten (10) seconds under normal operating conditions.

SecureTrust shall maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities and/or revoke a Certificate that is the subject of such a complaint. See also section 4.9.5.

4.10.3 Optional Features

Not applicable.

4.11 END OF SUBSCRIPTION

SecureTrust shall attempt to notify all Subscribers of the expiration date of their Certificate. Notifications will generally be by email 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, SecureTrust may not send expiration notices to that party. SecureTrust is not responsible for ensuring that the customer is notified prior to the expiration of their Certificate.

4.12 KEY ESCROW AND RECOVERY

SecureTrust does not provide nor perform any form of key escrow or recovery services.

4.12.1 Key Escrow and Recovery Policy and Practices

Not applicable.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site Location and Construction

SecureTrust's 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.

SecureTrust 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 biometric readers, proximity cards, and Keys. The system has been designed so that entry by a single Individual is not possible. On an annual basis, physical access to the CA room is audited by Trustwave internal audit for:

- Review of trusted individuals with key card access
- Date and time of entry
- Identity of the person making the journal entry
- Description of entry

5.1.3 Power and Air Conditioning

SecureTrust's facility is equipped with primary and backup:

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

5.1.4 Water Exposures

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

5.1.5 Fire Prevention and Protection

SecureTrust 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 SecureTrust 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 SecureTrust's normal waste disposal requirements.

5.1.8 Off-site Backup

SecureTrust 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 facility, located 26 miles away, for its CA operations.

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:

1. Customer service personnel;
2. Cryptographic business operations personnel;
3. Security personnel;
4. System administration personnel;
5. Designated engineering personnel; and
6. Executives that are designated to manage infrastructural trustworthiness.

SecureTrust 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. Before any person is placed in a Trusted Role the CA Operational Committee head for that particular role must approve the placement.

5.2.2 Number of Persons Required per Task

SecureTrust 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.

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

1. Issued access devices and granted access to the required facilities;
2. Issued electronic credentials to access and perform specific functions on SecureTrust's 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):

1. The Generation, Issuing, Backups, Or Destruction Of A Root CA Key Pair;
2. The Loading Of Root CA Keys On An HSM;
3. The Storage Of Or Access To Root CA Key Material; And

4. 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, SecureTrust 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, SecureTrust shall maintain the following practices:

1. SecureTrust shall provide all employees and contractors interacting with the SPH 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.
2. SecureTrust shall maintain all records associated with training of the employees and contractors within the SPH for seven years.
3. Individuals responsible for the progression of initially gathering, then validating, subsequently approving, and finally auditing information, associated with any Certificate issuance process, shall qualify for each skill level prior to advancing to the next. This qualification will consist of an internally administered examination.

5.3.2 Background Check Procedures

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

1. Social Security Number Verification;
2. Criminal Records Search;
3. Credit History Review;
4. Education Verification;
5. Employment History Verification; and
6. Foreign Records Search.

For all persons in a Trusted Role a background check will be performed every 18 months.

5.3.3 Training Requirements

SecureTrust 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 SPH in a role supporting extended validation shall undergo an annual retraining exercise.

5.3.5 Job Rotation Frequency and Sequence

All personnel performing validation duties (“Validation Specialists”) rotate as deemed appropriate.

5.3.6 Sanctions for Unauthorized Actions

Failure of any Trustwave employee or agent, affiliated to SecureTrust’s CA business, 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. SecureTrust has an internal mechanism to report and track any action pursuant to this section 5.3.6.

5.3.7 Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles interacting with any component of the SPH 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 SPH CA operations.

5.4 AUDIT LOGGING PROCEDURES

5.4.1 Types of Events Recorded

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

1. Compliance with this CP/CPS and other obligations under SecureTrust agreements with subscribers
2. All actions, information, and events material to the enrollment, creation, issuance, use, expiration, and revocation of all Certificates issued by SecureTrust

Specifically, SecureTrust shall record the following events:

1. CA key lifecycle management events, including:
    a. Key generation, backup, storage, recovery, archival, and destruction; and
    b. Cryptographic device lifecycle management events.
2. CA and Subscriber Certificate lifecycle management events, including:
    a. Certificate Requests, renewal requests, re-key requests, and revocation;
    b. All verification activities stipulated in the CA Browser Forum Baseline Requirements document and SecureTrust's CPS.
    c. Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    d. Acceptance and rejection of Certificate Requests;
    e. Issuance of Certificates; and
    f. Generation of Certificate Revocation Lists (CRLs) and OCSP entries.
3. Security events, including:
    a. Successful and unsuccessful PKI system access attempts;
    b. PKI and security system actions performed;
    c. Security profile changes;
    d. System crashes, hardware failures, and other anomalies;
    e. Firewall and router activities; and
    f. Entries to and exits from the SecureTrust physical CA facility.

5.4.2 Frequency of Processing Log

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

5.4.3 Retention Period for Audit Log

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

5.4.4 Protection of Audit Log

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

1. Network segregation
2. Network intrusion detection systems,
3. Network firewalls, and
4. Antivirus systems (where applicable).

In addition, SecureTrust 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

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

5.4.6 Audit Collection System (Internal vs. External)

Audit logs are collected throughout the uptime of applicable systems and protected to ensure integrity and availability and, where appropriate, confidentiality.

5.4.7 Notification to Event-Causing Subject

Events that are determined to be potential security issues are escalated for further investigation.

5.4.8 Vulnerability Assessments

The Trustwave Information Security Program includes technical information security controls and performs regular risk assessments (Risk Assessments), at least on an annual basis, that:

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

Trustwave performs quarterly vulnerability scanning across the SecureTrust managed certification authority infrastructure. Trustwave performs annual penetration testing.

5.5 RECORDS ARCHIVAL

5.5.1 Types of Records Archived

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

1. 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;
2. All appropriate documentation submitted by Applicants in support of a Certificate application;
3. All records associated with Certificate issuance as part of its Certificate;
    a. Approval checklist process
    b. The Subscriber's PKCS#10 CSR;
    c. Documentation of organizational existence for organizational applicants as listed in Section 3.2.2;
    d. Documentation of Individual identity for Individual Applicants;
    e. Verification of organizational existence and status received from third party databases and government entities (including screen shots of web sites reporting such information);
    f. Screen shot of WHOIS record for domain name to be listed in the Certificate;
    g. Mailing address validation (if different than those identified through the resources listed above);
    h. Letter of authorization for web sites managed by third party agents of Applicants (if applicable);
    i. Submission of the Certificate application, including acceptance of the Subscriber Agreement;
    j. Name, email, and IP address of person acknowledging authority of the Contract Signer and Approver;
    k. Other relevant contact information for the Applicant/Subscriber; and
    l. Copies of Digital Certificates issued.
4. Requests for Certificate revocation are recorded and archived, including the name of the person requesting revocation, the reason for the request and the SecureTrust personnel involved in authorizing revocation. This information is retained as records in electronic archives for the period detailed in Section 5.5.2 below

5.5.2 Retention Period for Archive

SecureTrust retains the records of all certification authority activities and the associated documentation for a term of no less than 7 years after the last Certificate based on that documentation expires.

5.5.3 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.

5.5.4 Archive Backup Procedures

SecureTrust maintains backup copies of its archived records at a separate location from its primary operations.

5.5.5 Requirements for Time-stamping of Records

All system time settings for all components within the SecureTrust managed SPH 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 with a UTC(k) time source.

5.5.6 Archive Collection System (Internal or External)

Archive information is collected internally by SecureTrust.

5.5.7 Procedures to Obtain and Verify Archive Information

After receiving a request for information, SecureTrust may elect to retrieve archived information in order to satisfy that request. In this case, SecureTrust will work in concert with its off-site vendor to retrieve said data.

5.6 KEY CHANGEOVER

SecureTrust 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 CRLs. A new CA signing key pair shall be commissioned, and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. When all of the remaining certificates issued from a key pair have been revoked or expired the related CA key pair shall be destroyed as per section 6.2.10 herein.

5.7 COMPROMISE AND DISASTER RECOVERY

5.7.1 Incident and Compromise Handling Procedures

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

1. Inform all Application Software Suppliers, Subscribers, and Relying Parties of which SecureTrust is aware.
2. Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

5.7.2 Computing Resources, Software, and/or Data are Corrupted

SecureTrust maintains backup hardware and will put it into service in the event of system failures affecting the CA systems. Regular backups of software and data are also performed and will be restored as warranted according to the situation. SecureTrust will make all reasonable efforts to restore full functionality in a minimum of time, with priority given to restoring certificate status and revocation capabilities if such have been affected by the corruption.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a CA operated by SecureTrust, Key Compromise Response procedures are enacted by the Security Incident Response Team. This team, which includes representatives from Trustwave Legal, Security, Compliance, IT, SSL Operations and SSL Engineering, assesses the situation, develops an action plan, and implements the action plan with approval from Trustwave executive management and the SecureTrust CPB.

1. Inform all Application Software Suppliers, Subscribers, and Relying Parties of which SecureTrust is aware.
2. Immediately revoke all certificates issued within that portion of the SPH by issuing final CRLs for all certification authorities underneath the compromised certification authority, and subsequently terminate issuing and distribution of Certificates and CRLs;
3. Request revocation of the compromised Certificate;
4. Destroy compromised CA private keys as per section 6.2.10 herein; and

5. Generate a new CA key pair and Certificate and publish the Certificate in the Repository.

5.7.4 Business Continuity Capabilities After a Disaster

SecureTrust maintains several documented disaster recovery and business continuity plans for use in the case of a declared disaster. All certification authorities managed by SecureTrust within the SPH shall adhere to and follow these plans in the case of a declared disaster associated with any certification authority. These plans are published under the internal Trustwave Business Continuity and Disaster Recovery internal policy as amended from time to time, at least once a year.

5.8 CA OR RA TERMINATION

In the event that SecureTrust ceases operating, SecureTrust shall make a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance. If practical, SecureTrust will develop a termination plan to minimize disruption to Subscribers and Relying Parties. Such termination plans may address the following, as applicable:

1. Provision of notice to parties affected by the termination, such as Application Software Suppliers, Subscribers, and Relying Parties;
2. Informing such parties of the status of the CA;
3. Handling the cost of such notice;
4. The preservation of the CA's archives and records for the time periods required in this CP/CPS;
5. The continuation of Subscriber and customer support services;
6. The continuation of revocation services, such as the issuance of CRLs;
7. The revocation of unexpired, unrevoked Certificates of Subscribers and subordinate CAs, if necessary;
8. 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;
9. Disposition of the CA's Private Key and the hardware tokens containing such Private Key;
10. Provisions needed for the transition of the CA's services to a successor CA; and
11. The identity of the custodian of SecureTrust'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 SecureTrust security and audit requirements guidelines and the CA/Browser Forum Guidelines in a trusted and highly secured environment with backup and key recovery procedures. 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 period of at least 7 years after the end of the Validity Period of the CA Key Pair.

When SecureTrust 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. SecureTrust 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 SecureTrust Certification Authority Key Pair Generation

All SecureTrust-owned and managed certification authority key pairs shall be:

1. Generated in hardware security modules as defined in section 6.2;
2. RSA key pairs shall be of at least 2048 bit size; ECDSA key pairs shall use the NIST P-256 or P-384 Curves;
3. Performed in accordance with a documented key generation 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 a period of at least 7 years after the end of the Validity Period for the generated Key Pair; and
4. Performed by multiple trusted and qualified Trustwave employees.

6.1.1.2 RA key pair generation

Not applicable.

6.1.1.3 Subscriber key pair generation

SecureTrust issues certificates for RSA and ECDSA keys. Subscriber-generated public keys are tested by SecureTrust to confirm that they meet the qualifications in section 6.1.5 and 6.1.6 prior to SecureTrust issuing a certificate containing those keys.

6.1.2 Private Key Delivery to Subscriber

SecureTrust does not perform Subscriber key pair generation. SecureTrust mandates storage of private keys for OV Code Signing certificates within hardware security modules for Subscribers but does not mandate this method of private key storage for other certificate types. SecureTrust does not perform private key delivery to Subscribers.

6.1.3 Public Key Delivery to Certificate Issuer

The subscriber delivers the public key to SecureTrust in the form of a PKCS#10 Certificate Signing Request (CSR). For a Client Authentication Certificate or S/MIME Certificate, the subscriber may alternatively deliver the public key in the form of a Signed Public Key and Challenge (SPKAC).

6.1.4 CA Public Key Delivery to Relying Parties

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

6.1.5 Key Sizes

All certification authorities within SPH, as well as all subscriber keys, shall use at least 2048-bit RSA keys with a modulus length evenly divisible by 8, NIST P-256, or P-384 curve ECC keys. SecureTrust periodically, at least annually, reviews SSL industry standards, including without limitation minimum key length.

6.1.6 Public Key Parameters Generation and Quality Checking

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

The public exponent of all subscriber RSA keys must have a value of 65,537. The public key of all subscriber ECDSA keys must pass verification using the ECC Full Public Key Validation Routine, as described in NIST SP 800-56A Revision 2 Section 5.6.2.3.2. Additional key quality checks on subscriber keys, including Debian and ROCA weak key checks, are performed as vulnerabilities are discovered.

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

All Certificates within the SPH shall contain the X.509 v3 keyUsage field, and, where appropriate, extended key usage extensions, so that the usage of the private key can be delimited and determined by X.509 compliant software. In addition, Subscriber Certificates must have extended key usage extensions set.

No Certificate within, or issued by any CA within, the SPH shall have the Non Repudiation (“nonRepudiation”) keyUsage bit present within the Certificate. See Table 3 for KU and EKU assignments.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

All private keys within the SecureTrust managed component of the SPH shall be protected via 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 SecureTrust managed SPH require a minimum of three trusted and qualified Trustwave employees to come together in order to derive the private key.

6.2.3 Private Key Escrow

SecureTrust does not, nor does it have the facilities to, escrow private keys.

6.2.4 Private Key Backup

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

All private key backups of the following global root certification authorities – SGCA, XGCA, STCA, TWGCA, TWGP256CA, and TWGP384CA shall be stored in hardware such that it requires three trusted and qualified Trustwave employees to come together in order to regenerate the private key.

6.2.5 Private Key Archival

SecureTrust does not archive private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

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

1. Performed in accordance with a documented key movement ceremony that is either audited by the current WebTrust auditor or videotaped. Following completion of the ceremony, all Trustwave employees present shall

attest in signatory form to the adherence of the procedure. These records shall be kept for at least 7 years after the end of the Validity Period of the transferred Key Pair(s); and
2. Performed by multiple (at least three) trusted and qualified Trustwave employees.

6.2.7 Private Key Storage on Cryptographic Module

See Section 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. SecureTrust maintains no role in the generation, protection, or maintenance of Subscriber private keys.

All SecureTrust managed SPH components require multiple trusted and qualified Trustwave employees (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 Deactivating Private Key

The private keys stored on hardware security modules are deactivated via the hosting operating systems when not in use. 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

Where required, SecureTrust destroys CA private keys in a manner that reasonably ensures that there are no residual remains of the key that could lead to the reconstruction of such key. This includes destruction of all on-line, backup and archived copies of the key material. SecureTrust utilizes the vendor approved zeroization function of its hardware cryptographic modules and other appropriate means to ensure the complete destruction of CA private keys. When performed, CA key destruction activities are logged. All key destruction activities are initiated through the Trustwave IT change management process and subjected to SecureTrust CPB approval. Only authorized personnel are permitted to perform key destruction operations.

6.2.11 Cryptographic Module Rating

See Section 6.2.1

6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1 Public Key Archival

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

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

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

1. Root CA –31 years (XGCA, STCA, SGCA, TWGCA, TWGP256CA, TWGP384CA)
    a. All newly generated root CAs must be created with an RSA key, modulus 4096, or an ECC key, NIST P-256 or P-384 curve, and set to expire after at most 25 years.
2. SecureTrust managed subordinate CA set to expire no later than the root CA from which it was issued.
    a. Unless technically constrained by extended key usage to either code signing or timestamping usage, all newly-generated SecureTrust managed subordinate CAs must be set to expire after at most 10 years.
3. EV SSL Certificates
    a. 27 months for certificates issued prior to March 1, 2018.
    b. 825 days for certificates issued on or after March 1, 2018 and prior to August 31, 2020.
    c. 398 days for certificates issued on or after August 31, 2020.
4. OV SSL and DV SSL Certificates –
    a. 39 months for certificates issued prior to March 1, 2018.
    b. 825 days for certificates issued on or after March 1, 2018 and prior to August 31, 2020.
    c. 398 days for certificates issued on or after August 31, 2020.
5. Timestamp Certificates – 135 months

6. OCSP Responder Certificates – 12 months
7. All other certificate types (including OV Code Signing Certificates) – 39 months

6.4 ACTIVATION DATA

SecureTrust 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, SecureTrust deploys a "n out of m" secret sharing routine for electronic access to CA private keys, where "m" is greater than two and "n" is five. In other words, three of the five 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 five 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 five 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 HSMs.

6.4.3 Other Aspects of Activation Data

Not Applicable.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

SecureTrust requires and enforces multi-factor authentication for all Validation Specialist accounts capable of directly causing certificate issuance, in order to further protect and secure computer accounts associated with our certificate business.

6.5.2 Computer Security Rating

Not Applicable.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

SecureTrust 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

SecureTrust maintains both technical and procedural mechanisms to monitor change to all components within the SPH.

6.6.3 Life Cycle Security Controls

SecureTrust regularly updates its internally-developed software and monitors developments in its externally-sourced software and hardware and updates as appropriate in order to protect against vulnerabilities and ensure that its systems and processes are properly protected.

6.7 NETWORK SECURITY CONTROLS

The systems containing SecureTrust's SPH 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 SecureTrust 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 SPH shall be documented and approved via a change management system.

SecureTrust's Root CA private keys (STCA, SGCA, XGCA, TWGCA, TWGP256CA, and TWGP384CA) are kept in an offline (not network-connected) state and powered down when not in use. In addition, the HSM holding these keys requires two trusted and qualified Trustwave employees to provide smart cards in order to perform signing operations using the keys. These keys are used exclusively for signing SecureTrust Subordinate CAs, OCSP responder certificates, and CRLs for the Root CAs.

6.8 TIME-STAMPING

SecureTrust offers a Trusted Timestamping service compliant with RFC 3161. The private keys used for signing Time Stamp Tokens are protected in the same manner as the private keys for the SecureTrust managed SPH described in Section 6.2. The clock used to generate the Trusted Timestamps is synchronized with a UTC(k) time source at least once per day.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

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

7.1.1 Version Number(s)

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

7.1.2 Certificate Extensions

7.1.2.1 Root Certification Authority Extensions

Extension Name	*Required / Optional*	*Criticality*	*Extension Value*
Basic Constraints	Required	Critical	CA: true
Key Usage	Required	Critical for all Certificates issued after January 1, 2013	Certificate Signing, CRL Signing, Digital Signature (optional)
CRL Distribution Points	Optional	Not critical	CRL URI

7.1.2.2 Subordinate Certification Authority Extensions

Extension Name	*Required / Optional*	*Criticality*	*Extension Value*
Basic Constraints	Required	Critical	CA: true, pathLen: 0 (for Certificates that issue End-Entity Certificates)
Key Usage	Required	Critical for all Certificates issued after January 1, 2013	Certificate Signing, CRL Signing, Digital Signature (optional)
Extended Key Usage	Required	Not critical	See Table 3
CRL Distribution Points	Required	Not critical	CRL URI
Authority Information Access	Required for Certificates issued after January 1, 2013 and/or issue End-Entity Certificates	Not critical	OCSP Responder URI, Issuing CA Certificate URI (optional)

7.1.2.3 Subscriber Certificate Extensions

7.1.2.3.1 SSL (DV, OV, EV) Subscriber Certificate Extensions

Extension Name	*Required / Optional*	*Criticality*	*Extension Value*
Basic Constraints	Required	Critical	CA: false
Key Usage	Required	Critical	See Table 3
Extended Key Usage	Required	Not critical	See Table 3
Subject Alternative Name	Required	Not critical	GeneralNames list
CRL Distribution Points	Required	Not critical	CRL URI
Authority Information Access	Required	Not critical	OCSP Responder URI, Issuing CA Certificate URI (optional)
Certificate Policies	Required	Not critical	See Table 2 for Policy OID(s)
Signed Certificate Timestamp	Optional	Not critical	One or more Signed Certificate Timestamps
TLS Feature	Optional	Not critical	Status Request (“OCSP Must-Staple”) feature

7.1.2.3.2 OV Code Signing Certificate Extensions

Extension Name	*Required / Optional*	*Criticality*	*Extension Value*
Basic Constraints	Required	Critical	CA: false
Key Usage	Required	Critical	See Table 3
Extended Key Usage	Required	Not critical	See Table 3
CRL Distribution Points	Required	Not critical	CRL URI
Authority Information Access	Required	Not critical	OCSP Responder URI, Issuing CA Certificate URI (optional)
Certificate Policies	Required	Not critical	See Table 2 for Policy OID(s)

7.1.2.3.3 Client Authentication Certificate Extensions

Extension Name	*Required / Optional*	*Criticality*	*Extension Value*
Basic Constraints	Required	Critical	CA: false
Key Usage	Required	Critical	See Table 3
Extended Key Usage	Required	Not critical	See Table 3
CRL Distribution Points	Required	Not critical	CRL URI
Authority Information Access	Required	Not critical	OCSP Responder URI, Issuing CA Certificate URI (optional)
Certificate Policies	Required	Not critical	See Table 2 for Policy OID(s)

7.1.2.3.4 S/MIME Certificate Extensions

Extension Name	*Required / Optional*	*Criticality*	*Extension Value*
Basic Constraints	Required	Critical	CA: false
Key Usage	Required	Critical	See Table 3
Extended Key Usage	Required	Not critical	See Table 3
CRL Distribution Points	Required	Not critical	CRL URI
Authority Information Access	Required	Not critical	OCSP Responder URI, Issuing CA Certificate URI
Certificate Policies	Required	Not critical	See Table 2 for Policy OID(s)

7.1.2.4 All Certificates

All Certificates issued by SecureTrust contain fields and extensions set in accordance with RFC 5280.

7.1.2.5 Application of RFC 5280

SecureTrust issues precertificates exclusively from precertificate signing Certificates. All precertificates and precertificate signing Certificates issued by SecureTrust are compliant with the specifications as defined in RFC 6962. In addition to the criteria specified in RFC 6962 section 3.1, SecureTrust's precertificate signing Certificates are issued exclusively by CAs containing a pathLen:0 constraint preventing their use as Certificate issuers. Neither of these objects are considered "Certificates" and are not subject to the requirements as defined in RFC 5280.

7.1.3 Algorithm Object Identifiers

All Certificates issued by Certification Authorities within the SPH are signed using one of the following algorithms:

1. sha256WithRSAEncryption
2. ecdsa-with-SHA256
3. ecdsa-with-SHA384

7.1.4 Name Forms

SecureTrust Certificates are populated using X.500 naming conventions.

7.1.4.1 Issuer Information

The content of the Certificate Issuer Distinguished Name field matches the Subject DN of the Issuing CA to support Name-Chaining as specified in RFC 5280, section 4.1.2.4.

7.1.4.2 Subject Information – Subscriber Certificates

All Subscriber Certificates are populated with Subject Information as defined in section 3.1.1.

7.1.4.3 Subject Information – Root Certificates and Subordinate CA Certificates

All Root and Subordinate CA Certificates contain Subject Information that has been verified to be accurate. At a minimum, the “commonName”, “organizationName”, and “countryName” subject fields are populated.

7.1.5 Name Constraints

SecureTrust constrains its subordinate CA certificates with Extended Key Usage (EKU) values limiting each CA to issuing only its intended types of certificates. SecureTrust does not employ the Name Constraints x.509 extension for further limiting certain subordinate CA certificates to issue only for certain domains.

7.1.6 Certificate Policy Object Identifier

7.1.6.1 Reserved Certificate Policy Identifers

SecureTrust may include Reserved Certificate Policy Identifer(s) in Subscriber Certificates and Subordinate CA Certificates. If SecureTrust asserts the Reserved Certificate Policy Identifer(s) in a Certificate, SecureTrust asserts that the Certificate was issued in compliance with the specified Certificate Policy.

7.1.6.2 Root CA Certificates

SecureTrust does not add the certificatePolicies extension to Root CA Certificates.

7.1.6.3 Subordinate CA Certificates

SecureTrust may assert the following Certificate Policy OID(s) in Subordinate CA Certificates:

1. The “anyPolicy” identifier (2.5.3.29.32.0); or
2. The set of Certificate Policy OID(s) asserted in Subscriber Certificates to be issued from the Subordinate CA, as specified in section 1.2, Table 2

7.1.6.4 Subscriber Certificates

SecureTrust asserts the Certificate Policy OID(s) in all Subscriber Certificates as specified in Section 1.2, Table 2.

7.1.7 Usage of Policy Constraints Extension

SecureTrust does not include the Policy Constraints extension in any of the certificates within the SPH.

7.1.8 Policy Qualifiers Syntax and Semantics

SecureTrust includes the id-qt-cps qualifier in its certificates which contains a URI from which this document can be obtained.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Not applicable.

7.2 CRL PROFILE

For each of the certification authorities owned and managed by SecureTrust within the SPH, CRLs conforming to RFC 5280 shall be regularly issued in accordance with section 4.9.7, containing:

1. Version (set to “1” in order to indicate version 2);
2. Issuer Signature Algorithm, which is one of the following:
    a. sha1WithRSAEncryption, but only if the certification authority has issued Certificates signed with sha1WithRSAEncryption
    b. sha256WithRSAEncryption
    c. ecdsa-with-SHA256
    d. ecdsa-with-SHA384;
3. Issuer Distinguished Name (the issuing certification authority);

4. This Update in ISO 8601 format with UTC designation;
5. Next Update in ISO 8601 format with UTC designation;
6. The list of revoked Certificates, including the corresponding reason code for each revocation (required for revoked Issuing CA Certificates; optional otherwise);
7. Serial Number;
8. Revocation Date;
9. Signature of the CRL.

7.2.1 Version Number(s)

SecureTrust issues version 2 CRLs for all certification authorities within the SPH.

7.2.2 CRL and CRL Entry Extensions

Each Certificate revocation list issued by SecureTrust may contain:

1. CRL Number (unique);
2. Authority Key Identifier;
3. CRL Entry Extensions;
4. Invalidity Date (UTC - optional); and
5. Reason Code (required where the revocation entry corresponds to an Issuing CA Certificate; optional otherwise).

7.3 OCSP PROFILE

SecureTrust operates an OCSP service at http://ocsp.securetrust.com/. SecureTrust's OCSP responders conform to version 1 of IETF RFC 5019 and/or RFC 6960.

7.3.1 Version Number(s)

OCSP responses issued by SecureTrust shall use version 1 as defined within IETF RFC 5019 and/or RFC 6960.

7.3.2 OCSP Extensions

Appropriate extensions from RFC 5019 and/or RFC 6960 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

SecureTrust and all components of the SPH SHALL:

1. Comply with applicable laws;
2. Comply with the requirements of this Certificate Policy and Certification Practice Statement; and
3. Comply with the requirements of the then-current WebTrust program for CAs (latest relevant version) completed by a licensed WebTrust for CAs auditor.

An annual audit is performed by an independent external auditor to assess SecureTrust'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. SecureTrust undergoes yearly audits using CPA Canada WebTrust for certification authorities, including extended validation criteria, for all components of the SecureTrust managed SPH and complies with all requirements of the program.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

SecureTrust shall conduct the CPA Canada WebTrust audits, including extended validation criteria, on a yearly basis.

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

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

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

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

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The public accounting firm that conducts the CPA Canada WebTrust audits for SecureTrust shall be completely independent of Trustwave.

8.4 TOPICS COVERED BY ASSESSMENT

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

1. CA business practices disclosure
2. Detailed validation process
3. Service integrity
4. CA environmental controls.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6 COMMUNICATION OF RESULTS

All results of the WebTrust audit for SecureTrust 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. SecureTrust audit reports are available from WebTrust by clicking on the WebTrust seal on our homepage, https://certs.securetrust.com/, or by visiting SecureTrust's Repository at https://certs.securetrust.com/CA.

8.7 AUDIT REQUIREMENTS

8.7.1 Pre-Issuance Readiness Audit

1. If SecureTrust 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 SecureTrust MUST successfully complete a point-in-time readiness assessment audit against equivalent audit procedures approved by the CA/Browser Forum.
2. If SecureTrust 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 SecureTrust MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program, or an equivalent as approved by the CA/Browser Forum.

8.7.2 Regular Self Audits

During the period in which it issues SSL Certificates, SecureTrust MUST strictly control its service quality by performing ongoing self-audits against a randomly selected sample of at least three percent of the SSL 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 due diligence requirements of Section 11.13 of the EV Guidelines is performed by an RA, SecureTrust 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.

SecureTrust annually internally audits compliance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates.

8.7.3 Annual Independent Audit

During the period in which it issues SSL Certificates, SecureTrust must undergo and pass an annual (i) WebTrust Program for CAs audit, (ii) WebTrust Baseline audit, (iii) WebTrust EV Program audit, and (iv) WebTrust Code Signing audit or an equivalent for all (i), (ii), (iii), and (iv) 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 SecureTrust 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:

1. 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
2. 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
3. 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, SecureTrust'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 root keys produced. The Qualified Auditor MUST then issue a report opining that SecureTrust, during its root key and certificate generation process:

1. Documented its Root CA key generation and protection and procedures in its Certificate Policy, and its Certification Practices Statement, (CP and CPS);
2. 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;
3. 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.
4. 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

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

9.1.2 Certificate Access Fees

SecureTrust 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

SecureTrust does not charge a fee for access to revocation information in the form of CRLs or OCSP services. SecureTrust may, in its discretion, charge a fee to provide customized CRLs or status information in non-standard formats.

9.1.4 Fees for Other Services

SecureTrust 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

SecureTrust's refund policy may be found at https://certs.securetrust.com/CA.

9.2 FINANCIAL RESPONSIBILITY

9.2.1 Insurance Coverage

SecureTrust encourages customers, Subscribers, End-Entities, Relying Parties, and all other entities to maintain adequate insurance to protect against errors and omissions, professional liability, and general liability. SecureTrust currently maintains commercially reasonable insurance with a Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage.

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

SecureTrust's warranty coverage for Relying Parties may be found at https://certs.securetrust.com/CA.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

The following Subscriber documentation shall be maintained in confidence.

1. CA application records, whether approved or disapproved;
2. Certificate Application records;
3. Subscriber Agreement
4. Private keys held by customers and subscribers and information needed to recover such Private Keys;
5. Transactional records;
6. Contingency planning and disaster recovery plans; and
7. Security measures controlling the operations of SecureTrust's 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:

1. Certificates;
2. Certificate revocation;
3. Certificate status; and
4. SecureTrust repositories and their contents.

9.3.3 Responsibility to Protect Confidential Information

SecureTrust protects and secures confidential information from disclosure.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

Trustwave's privacy plan/policy may be found at the following location: https://www.trustwave.com/en-us/legal-documents/privacy-policy/.

9.4.2 Information Treated as Private

Non-public Subscriber information is treated as private.

9.4.3 Information Not Deemed Private

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

9.4.4 Responsibility to Protect Private Information

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

9.4.5 Notice and Consent to Use Private Information

Unless otherwise stated in this 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.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

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

9.4.7 Other Information Disclosure Circumstances

Refer to section 9.4.6.

9.5 INTELLECTUAL PROPERTY RIGHTS

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

1. This CPS and CPs;
2. Certificates;
3. Revocation Information;
4. Trustwave's logos, trademarks and service marks; and

5. Trustwave's root keys and the root Certificates containing them.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

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

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

9.6.2 RA Representations and Warranties

RAs warrant that, to the best of their knowledge:

1. there are no material misrepresentations of fact with the Certificates;
2. there are no errors in the information within the Certificates caused by the RA's failure to exercise reasonable care in approving, creating, issuing, and managing the Certificates; and
3. the Certificates comply with the material requirements of this CPS and the applicable CPs.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

1. 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;
2. Their private key is protected and that no unauthorized person has ever had access to the Subscriber's private key;
3. All representations made by the Subscriber in the Certificate Application the Subscriber submitted are true;
4. All information supplied by the Subscriber and contained in the Certificate is true;
5. The Certificate is being used exclusively for authorized and legal purposes consistent with this CP/CPS, and
6. 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.
7. No subscriber private key associated with any certificate issued within the SecureTrust public key infrastructure shall be used to affix a digital signature to any document, contract, or letter.

Subscriber Agreements may include additional representations and warranties.

9.6.4 Relying Party Representations and Warranties

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

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

Not applicable.

9.7 DISCLAIMERS OF WARRANTIES

EXCEPT FOR THE LIMITED WARRANTY DESCRIBED HEREIN AND TO THE GREATEST EXTENT PERMITTED BY APPLICABLE LAW, TRUSTWAVE EXPRESSLY DISCLAIMS AND MAKES NO REPRESENTATION, WARRANTY OR COVENANT OF ANY KIND, WHETHER EXPRESS OR IMPLIED, EITHER IN FACT OR BY OPERATION OF LAW, WITH

RESPECT TO THIS 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.

9.8 LIMITATIONS OF LIABILITY

IN NO EVENT SHALL THE CUMULATIVE OR AGGREGATE LIABILITY OF TRUSTWAVE TO ANY PARTY, INCLUDING WITHOUT LIMITATION TO APPLICANTS, SUBSCRIBER AND/OR ANY RELYING PARTY, FOR ALL CLAIMS 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).

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.

9.9 INDEMNITIES

9.9.1 Indemnification by Trustwave

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, Trustwave understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with Trustwave do not assume any obligation or potential liability of Trustwave under this CP/CPS or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Trustwave shall not be liable to Application Software Supplier for any claim, damages, or loss suffered by an Application Software Supplier related to a Certificate issued by Trustwave where such claim, damage, or loss was directly caused by such Application Software Supplier’s software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from Trustwave online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify Trustwave and its affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partners, successors and assigns) against any loss, damage, or expense, including reasonable attorney’s fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber’s breach of the Subscriber Agreement, this CP/CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber’s negligence or intentional acts; or (iv) Subscriber’s misuse of the Certificate or Private Key.

9.9.3 Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify Trustwave and its affiliates (including, but not limited to, its parent company, officers, directors, employees, agents, partners, successors and assigns) against any loss, damage, or expense, including reasonable attorney’s fees, related to the Relying Party’s (i) breach of the Relying Party Agreement, an End-User License Agreement, this CP/CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate’s status prior to use.

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

9.10 TERM AND TERMINATION

9.10.1 Term

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

9.10.2 Termination

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

9.10.3 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.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Refer to Section 1.5.4 hereof.

9.12.2 Notification Mechanism and Period

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

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

9.12.3 Circumstances under Which OID Must be Changed

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

9.13 DISPUTE RESOLUTION PROVISIONS

Any dispute, controversy or claim, which cannot be mutually resolved within ninety (90) days, arising under, in connection with or relating to this CPS the applicable CPs, SecureTrust's Websites, or any Certificate issued by SecureTrust 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 SecureTrust shall remain in full force and effect pending the outcome and award in any arbitration proceeding hereunder. In any arbitration arising

hereunder, each party to the preceding shall be responsible for its own costs incurred in connection with the arbitration proceedings, unless the arbitrator determines that the prevailing party is entitled to an award of all or a portion of such costs, including reasonable attorneys' fees actually incurred.

9.14 GOVERNING LAW

The enforceability, construction, interpretation, and validity of this CPS, the applicable CPs and any Certificates issued by SecureTrust shall be governed by the substantive laws of the State of Delaware, United States of America, excluding (i) the conflicts of law provisions thereof and (ii) the United Nations Convention on Contracts for the International Sale of Goods. Applicants, Subscribers, and Relying Parties irrevocably consent to jurisdiction in the State of Illinois and any and all actions against Trustwave or its affiliated companies shall be brought in the State of Illinois.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS and the applicable 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.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 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.

9.16.2 Assignment

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

9.16.3 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.

9.16.4 Enforcement (Attorneys' Fees and Waiver of Rights)

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

9.16.5 Force Majeure

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

9.17 OTHER PROVISIONS

Not applicable.

Appendix A: SecureTrust Root Certificates

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
                Public-Key: (2048 bit)
                Modulus:
                    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:

                Full Name:
                  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-----
```

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
                Public-Key: (2048 bit)
                Modulus:
                    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:

                Full Name:
                  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-----
```

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
                Public-Key: (2048 bit)
                Modulus:
                    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:

                Full Name:
                  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-----
```

TWGCA – TRUSTWAVE GLOBAL CERTIFICATION AUTHORITY

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            05:f7:0e:86:da:49:f3:46:35:2e:ba:b2
    Signature Algorithm: sha256WithRSAEncryption
        Issuer: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc.,
                CN=Trustwave Global Certification Authority
        Validity
            Not Before: Aug 23 19:34:12 2017 GMT
            Not After : Aug 23 19:34:12 2042 GMT
        Subject: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc.,
                 CN=Trustwave Global Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                Public-Key: (4096 bit)
                Modulus:
                    00:b9:5d:51:28:4b:3c:37:92:d1:82:ce:bd:1d:bd:
                    cd:dd:b8:ab:cf:0a:3e:e1:5d:e5:dc:aa:09:b9:57:
                    02:3e:e6:63:61:df:f2:0f:82:63:ae:a3:f7:ac:73:
                    d1:7c:e7:b3:0b:af:08:00:09:59:7f:cd:29:2a:88:
                    93:87:17:18:80:ed:88:b2:b4:b6:10:1f:2d:d6:5f:
                    55:a2:13:5d:d1:c6:eb:06:56:89:88:fe:ac:32:9d:
                    fd:5c:c3:05:c7:6e:ee:86:89:ba:88:03:9d:72:21:
                    86:90:ae:8f:03:a5:dc:9f:88:28:cb:a3:92:49:0f:
                    ec:d0:0f:e2:6d:44:4f:80:6a:b2:d4:e7:a0:0a:53:
                    01:ba:8e:97:91:76:6e:bc:fc:d5:6b:36:e6:40:88:
                    d6:7b:2f:5f:05:e8:2c:6d:11:f3:e7:b2:be:92:44:
                    4c:d2:97:a4:fe:d2:72:81:43:07:9c:e9:11:3e:f5:
                    8b:1a:59:7d:1f:68:58:dd:04:00:2c:96:f3:43:b3:
                    7e:98:19:74:d9:9c:73:d9:18:be:41:c7:34:79:d9:
                    f4:62:c2:43:b9:b3:27:b0:22:cb:f9:3d:52:c7:30:
                    47:b3:c9:3e:b8:6a:e2:e7:e8:81:70:5e:42:8b:4f:
                    26:a5:fe:3a:c2:20:6e:bb:f8:16:8e:cd:0c:a9:b4:
                    1b:6c:76:10:e1:58:79:46:3e:54:ce:80:a8:57:09:
                    37:29:1b:99:13:8f:0c:c8:d6:2c:1c:fb:05:e8:08:
                    95:3d:65:46:dc:ee:cd:69:e2:4d:8f:87:28:4e:34:
                    0b:3e:cf:14:d9:bb:dd:b6:50:9a:ad:77:d4:19:d6:
                    da:1a:88:c8:4e:1b:27:75:d8:b2:08:f1:ae:83:30:
                    b9:11:0e:cd:87:f0:84:8d:15:72:7c:a1:ef:cc:f2:
                    88:61:ba:f4:69:bb:0c:8c:0b:75:57:04:b8:4e:2a:
                    14:2e:3d:0f:1c:1e:32:a6:62:36:ee:66:e2:22:b8:
                    05:40:63:10:22:f3:33:1d:74:72:8a:2c:f5:39:29:
                    a0:d3:e7:1b:80:84:2d:c5:3d:e3:4d:b1:fd:1a:6f:
                    ba:65:07:3b:58:ec:42:45:26:fb:d8:da:25:72:c4:
                    f6:00:b1:22:79:bd:e3:7c:59:62:4a:9c:05:6f:3d:
                    ce:e6:d6:47:63:99:c6:24:6f:72:12:c8:ac:7f:90:
                    b4:0b:91:70:e8:b7:e6:16:10:71:17:ce:de:06:4f:
                    48:41:7d:35:4a:a3:89:f2:c9:4b:7b:41:11:6d:67:
                    b7:08:98:4c:e5:11:19:ae:42:80:dc:fb:90:05:d4:
                    f8:50:ca:be:e4:ad:c7:c2:94:d7:16:9d:e6:17:8f:
                    af:36:fb
                Exponent: 65537 (0x10001)
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Subject Key Identifier:
                99:E0:19:67:0D:62:DB:76:B3:DA:3D:B8:5B:E8:FD:42:D2:31:0E:87
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
    Signature Algorithm: sha256WithRSAEncryption
```

```
        98:73:70:e2:b0:d3:ed:39:ec:4c:60:d9:a9:12:86:17:1e:96:
        d0:e8:54:28:3b:64:2d:21:a6:f8:9d:56:13:6a:48:3d:4f:c7:
        3e:29:db:6d:58:83:54:3d:87:7d:23:05:d4:e4:1c:dc:e8:38:
        65:86:c5:75:a7:5a:db:35:05:bd:77:de:bb:29:37:40:05:07:
        c3:94:52:9f:ca:64:dd:f1:1b:2b:dc:46:0a:10:02:31:fd:4a:
        68:0d:07:64:90:e6:1e:f5:2a:a1:a8:bb:3c:5d:f9:a3:08:0b:
        11:0c:f1:3f:2d:10:94:6f:fe:e2:34:87:83:d6:cf:e5:1b:35:
        6d:d2:03:e1:b0:0d:a8:a0:aa:46:27:82:36:a7:15:b6:08:a6:
        42:54:57:b6:99:5a:e2:0b:79:90:d7:57:12:51:35:19:88:41:
        68:25:d4:37:17:84:15:fb:01:72:dc:95:de:52:26:20:98:26:
        e2:76:f5:27:6f:fa:00:3b:4a:61:d9:0d:cb:51:93:2a:fd:16:
        06:96:a7:23:9a:23:48:fe:51:bd:b6:c4:b0:b1:54:ce:de:6c:
        41:ad:16:67:7e:db:fd:38:cd:b9:38:4e:b2:c1:60:cb:9d:17:
        df:58:9e:7a:62:b2:26:8f:74:95:9b:e4:5b:1d:d2:0f:dd:98:
        1c:9b:59:b9:23:d3:31:a0:a6:ff:38:dd:cf:20:4f:e9:58:56:
        3a:67:c3:d1:f6:99:99:9d:ba:36:b6:80:2f:88:47:4f:86:bf:
        44:3a:80:e4:37:1c:a6:ba:ea:97:98:11:d0:84:62:47:64:1e:
        aa:ee:40:bf:34:b1:9c:8f:4e:e1:f2:92:4f:1f:8e:f3:9e:97:
        de:f3:a6:79:6a:89:71:4f:4b:27:17:48:fe:ec:f4:50:0f:4f:
        49:7d:cc:45:e3:bd:7a:40:c5:41:dc:61:56:27:06:69:e5:72:
        41:81:d3:b6:01:89:a0:2f:3a:72:79:fe:3a:30:bf:41:ec:c7:
        62:3e:91:4b:c7:d9:31:76:42:f9:f7:3c:63:ec:26:8c:73:0c:
        7d:1a:1d:ea:a8:7c:87:a8:c2:27:7c:e1:33:41:0f:cf:cf:fc:
        00:a0:22:80:9e:4a:a7:6f:00:b0:41:45:b7:22:ca:68:48:c5:
        42:a2:ae:dd:1d:f2:e0:6e:4e:05:58:b1:c0:90:16:2a:a4:3d:
        10:40:be:8f:62:63:83:a9:9c:82:7d:2d:02:e9:83:30:7c:cb:
        27:c9:fd:1e:66:00:b0:2e:d3:21:2f:8e:33:16:6c:98:ed:10:
        a8:07:d6:cc:93:cf:db:d1:69:1c:e4:ca:c9:e0:b6:9c:e9:ce:
        71:71:de:6c:3f:16:a4:79
-----BEGIN CERTIFICATE-----
MIIF2jCCA8KgAwIBAgIMBfcOhtpJ80Y1LrqyMA0GCSqGSIb3DQEBCwUAMIGIMQsw
CQYDVQQGEwJVUzERMA8GA1UECAwISWxsaW5vaXMxEDAOBgNVBAcMB0NoaWNhZ28x
ITAfBgNVBAoMGFRydXN0d2F2ZSBIb2xkaW5ncywgSW5jLjExMC8GA1UEAwwoVHJ1
c3R3YXZlIEdsb2JhbCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0xNzA4MjMx
OTM0MTJaFw00MjA4MjMxOTM0MTJaMIGIMQswCQYDVQQGEwJVUzERMA8GA1UECAwI
SWxsaW5vaXMxEDAOBgNVBAcMB0NoaWNhZ28xITAfBgNVBAoMGFRydXN0d2F2ZSBI
b2xkaW5ncywgSW5jLjExMC8GA1UEAwwoVHJ1c3R3YXZlIEdsb2JhbCBDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eTCCAiIwDQYJKoZIhvcNAQEBBQADggIPADCCAgoCggIB
ALldUShLPDeS0YLOvR29zd24q88KPuFd5dyqCblXAj7mY2Hf8g+CY66j96xz0Xzn
swuvCAAJWX/NKSqIk4cXGIDtiLK0thAfLdZfVaITXdHG6wZWiYj+rDKd/VzDBcdu
7oaJuogDnXIhhpCujwOl3J+IKMujkkkP7NAP4m1ET4BqstTnoApTAbqOl5F2brz8
1Ws25kCI1nsvXwXoLG0R8+eyvpJETNKXpP7ScoFDB5zpET71ixpZfR9oWN0EACyW
80OzfpgZdNmcc9kYvkHHNHnZ9GLCQ7mzJ7Aiy/k9UscwR7PJPrhq4ufogXBeQotP
JqX+OsIgbrv4Fo7NDKm0G2x2EOFYeUY+VM6AqFcJNykbmROPDMjWLBz7BegIlT1l
RtzuzWniTY+HKE40Cz7PFNm73bZQmq131BnW2hqIyE4bJ3XYsgjxroMwuREOzYfw
hI0Vcnyh78zyiGG69Gm7DIwLdVcEuE4qFC49DxweMqZiNu5m4iK4BUBjECLzMx10
coos9TkpoNPnG4CELcU9402x/RpvumUHO1jsQkUm+9jaJXLE9gCxInm943xZYkqc
BW89zubWR2OZxiRvchLIrH+QtAuRcOi35hYQcRfO3gZPSEF9NUqjifLJS3tBEW1n
twiYTOURGa5CgNz7kAXU+FDKvuStx8KU1xad5hePrzb7AgMBAAGjQjBAMA8GA1Ud
EwEB/wQFMAMBAf8wHQYDVR0OBBYEFJngGWcNYtt2s9o9uFvo/ULSMQ6HMA4GA1Ud
DwEB/wQEAwIBBjANBgkqhkiG9w0BAQsFAAOCAgEAmHNw4rDT7TnsTGDZqRKGFx6W
0OhUKDtkLSGm+J1WE2pIPU/HPinbbViDVD2HfSMF1OQc3Og4ZYbFdada2zUFvXfe
uyk3QAUHw5RSn8pk3fEbK9xGChACMf1KaA0HZJDmHvUqoai7PF35owgLEQzxPy0Q
lG/+4jSHg9bP5Rs1bdID4bANqKCqRieCNqcVtgimQlRXtpla4gt5kNdXElE1GYhB
aCXUNxeEFfsBctyV3lImIJgm4nb1J2/6ADtKYdkNy1GTKv0WBpanI5ojSP5RvbbE
sLFUzt5sQa0WZ37b/TjNuThOssFgy50X31ieemKyJo90lZvkWx3SD92YHJtZuSPT
MaCm/zjdzyBP6VhWOmfD0faZmZ26NraAL4hHT4a/RDqA5Dccprrql5gR0IRiR2Qe
qu5AvzSxnI9O4fKSTx+O856X3vOmeWqJcU9LJxdI/uz0UA9PSX3MReO9ekDFQdxh
VicGaeVyQYHTtgGJoC86cnn+OjC/QezHYj6RS8fZMXZC+fc8Y+wmjHMMfRod6qh8
h6jCJ3zhM0EPz8/8AKAigJ5Kp28AsEFFtyLKaEjFQqKu3R3y4G5OBVixwJAWKqQ9
EEC+j2Jjg6mcgn0tAumDMHzLJ8n9HmYAsC7TIS+OMxZsmO0QqAfWzJPP29FpHOTK
```

```
yeC2nOnOcXHebD8WpHk=
-----END CERTIFICATE-----
```

TWGP256CA – TRUSTWAVE GLOBAL ECC P256 CERTIFICATION AUTHORITY

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            0d:6a:5f:08:3f:28:5c:3e:51:95:df:5d
    Signature Algorithm: ecdsa-with-SHA256
        Issuer: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc.,
                CN=Trustwave Global ECC P256 Certification Authority
        Validity
            Not Before: Aug 23 19:35:10 2017 GMT
            Not After : Aug 23 19:35:10 2042 GMT
        Subject: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc.,
                 CN=Trustwave Global ECC P256 Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (256 bit)
                pub:
                    04:7e:fb:6c:e6:23:e3:73:32:08:ca:60:e6:53:9c:
                    ba:74:8d:18:b0:78:90:52:80:dd:38:c0:4a:1d:d1:
                    a8:cc:93:a4:97:06:38:ca:0d:15:62:c6:8e:01:2a:
                    65:9d:aa:df:34:91:2e:81:c1:e4:33:92:31:c4:fd:
                    09:3a:a6:3f:ad
                ASN1 OID: prime256v1
                NIST CURVE: P-256
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                A3:41:06:AC:90:6D:D1:4A:EB:75:A5:4A:10:99:B3:B1:A1:8B:4A:F7
    Signature Algorithm: ecdsa-with-SHA256
         30:44:02:20:07:e6:54:da:0e:a0:5a:b2:ae:11:9f:87:c5:b6:
         ff:69:de:25:be:f8:a0:b7:08:f3:44:ce:2a:df:08:21:0c:37:
         02:20:2d:26:03:a0:05:bd:6b:d1:f6:5c:f8:65:cc:86:6d:b3:
         9c:34:48:63:84:09:c5:8d:77:1a:e2:cc:9c:e1:74:7b
-----BEGIN CERTIFICATE-----
MIICYDCCAgegAwIBAgIMDWpfCD8oXD5Rld9dMAoGCCqGSM49BAMCMIGRMQswCQYD
VQQGEwJVUzERMA8GA1UECBMISWxsaW5vaXMxEDAOBgNVBAcTB0NoaWNhZ28xITAf
BgNVBAoTGFRydXN0d2F2ZSBIb2xkaW5ncywgSW5jLjE6MDgGA1UEAxMxVHJ1c3R3
YXZlIEdsb2JhbCBFQ0MgUDI1NiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0x
NzA4MjMxOTM1MTBaFw00MjA4MjMxOTM1MTBaMIGRMQswCQYDVQQGEwJVUzERMA8G
A1UECBMISWxsaW5vaXMxEDAOBgNVBAcTB0NoaWNhZ28xITAfBgNVBAoTGFRydXN0
d2F2ZSBIb2xkaW5ncywgSW5jLjE6MDgGA1UEAxMxVHJ1c3R3YXZlIEdsb2JhbCBF
Q0MgUDI1NiBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTBZMBMGByqGSM49AgEGCCqG
SM49AwEHA0IABH77bOYj43MyCMpg5lOcunSNGLB4kFKA3TjASh3RqMyTpJcGOMoN
FWLGjgEqZZ2q3zSRLoHB5DOSMcT9CTqmP62jQzBBMA8GA1UdEwEB/wQFMAMBAf8w
DwYDVR0PAQH/BAUDAwcGADAdBgNVHQ4EFgQUo0EGrJBt0UrrdaVKEJmzsaGLSvcw
CgYIKoZIzj0EAwIDRwAwRAIgB+ZU2g6gWrKuEZ+Hxbb/ad4lvvigtwjzRM4q3wgh
DDcCIC0mA6AFvWvR9lz4ZcyGbbOcNEhjhAnFjXca4syc4XR7
-----END CERTIFICATE-----
```

TWGP384CA – TRUSTWAVE GLOBAL ECC P384 CERTIFICATION AUTHORITY

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            08:bd:85:97:6c:99:27:a4:80:68:47:3b
    Signature Algorithm: ecdsa-with-SHA384
        Issuer: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc.,
                CN=Trustwave Global ECC P384 Certification Authority
        Validity
            Not Before: Aug 23 19:36:43 2017 GMT
            Not After : Aug 23 19:36:43 2042 GMT
        Subject: C=US, ST=Illinois, L=Chicago, O=Trustwave Holdings, Inc.,
                 CN=Trustwave Global ECC P384 Certification Authority
        Subject Public Key Info:
            Public Key Algorithm: id-ecPublicKey
                Public-Key: (384 bit)
                pub:
                    04:6b:da:0d:75:35:08:31:47:05:ae:45:99:55:f1:
                    11:13:2e:4a:f8:10:31:23:a3:7e:83:d3:7f:28:08:
                    3a:26:1a:3a:cf:97:82:1f:80:b7:27:09:8f:d1:8e:
                    30:c4:0a:9b:0e:ac:58:04:ab:f7:36:7d:94:23:a4:
                    9b:0a:8a:8b:ab:eb:fd:39:25:66:f1:5e:fe:8c:ae:
                    8d:41:79:9d:09:60:ce:28:a9:d3:8a:6d:f3:d6:45:
                    d4:f2:98:84:38:65:a0
                ASN1 OID: secp384r1
                NIST CURVE: P-384
        X509v3 extensions:
            X509v3 Basic Constraints: critical
                CA:TRUE
            X509v3 Key Usage: critical
                Certificate Sign, CRL Sign
            X509v3 Subject Key Identifier:
                55:A9:84:89:D2:C1:32:BD:18:CB:6C:A6:07:4E:C8:E7:9D:BE:82:90
    Signature Algorithm: ecdsa-with-SHA384
         30:64:02:30:37:01:92:97:45:12:7e:a0:f3:3e:ad:19:3a:72:
         dd:f4:50:93:03:12:be:44:d2:4f:41:a4:8c:9c:9d:1f:a3:f6:
         c2:92:e7:48:14:fe:4e:9b:a5:91:57:ae:c6:37:72:bb:02:30:
         67:25:0a:b1:0c:5e:ee:a9:63:92:6f:e5:90:0b:fe:66:22:ca:
         47:fd:8a:31:f7:83:fe:7a:bf:10:be:18:2b:1e:8f:f6:29:1e:
         94:59:ef:8e:21:37:cb:51:98:a5:6e:4b
-----BEGIN CERTIFICATE-----
MIICnTCCAiSgAwIBAgIMCL2Fl2yZJ6SAaEc7MAoGCCqGSM49BAMDMIGRMQswCQYD
VQQGEwJVUzERMA8GA1UECBMISWxsaW5vaXMxEDAOBgNVBAcTB0NoaWNhZ28xITAf
BgNVBAoTGFRydXN0d2F2ZSBIb2xkaW5ncywgSW5jLjE6MDgGA1UEAxMxVHJ1c3R3
YXZlIEdsb2JhbCBFQ0MgUDM4NCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0x
NzA4MjMxOTM2NDNaFw00MjA4MjMxOTM2NDNaMIGRMQswCQYDVQQGEwJVUzERMA8G
A1UECBMISWxsaW5vaXMxEDAOBgNVBAcTB0NoaWNhZ28xITAfBgNVBAoTGFRydXN0
d2F2ZSBIb2xkaW5ncywgSW5jLjE6MDgGA1UEAxMxVHJ1c3R3YXZlIEdsb2JhbCBF
Q0MgUDM4NCBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTB2MBAGByqGSM49AgEGBSuB
BAAiA2IABGvaDXU1CDFHBa5FmVXxERMuSvgQMSOjfoPTfygIOiYaOs+Xgh+AtycJ
j9GOMMQKmw6sWASr9zZ9lCOkmwqKi6vr/TklZvFe/oyujUF5nQlgziip04pt89ZF
1PKYhDhloKNDMEEwDwYDVR0TAQH/BAUwAwEB/zAPBgNVHQ8BAf8EBQMDBwYAMB0G
A1UdDgQWBBRVqYSJ0sEyvRjLbKYHTsjnnb6CkDAKBggqhkjOPQQDAwNnADBkAjA3
AZKXRRJ+oPM+rRk6ct30UJMDEr5E0k9BpIycnR+j9sKS50gU/k6bpZFXrsY3crsC
MGclCrEMXu6pY5Jv5ZAL/mYiykf9ijH3g/56vxC+GCsej/YpHpRZ744hN8tRmKVu
Sw==
-----END CERTIFICATE-----
```