CERTISIGN TRUST NETWORK CERTIFICATE POLICY

VERSION 1.6

FEV, 06 , 2019

CERTISIGN TRUST NETWORK
CERTIFICATE POLICY

Summary

CERTISIGN TRUST NETWORK
CERTIFICATE POLICY

1. Introduction

This document, "CERTISIGN TRUST NETWORK Certificate Policies" (CP) is the principal statement of policy governing CERTISIGN TRUST NETWORK. The CP sets forth the business, legal, and technical requirements forapproving, issuing, managing, using, revoking, and renewing, digital Certificates within CERTISIGN TRUST NETWORK and providing associated trust services for all participants within CERTISIGN TRUST NETWORK. These requirements protect the security and integrity of CERTISIGN TRUST NETWORK and comprise a single set of rules that apply widly, thereby providing assurances of uniform trust throughout CERTISIGN TRUST NETWORK. The CP is not a legal agreement between CERTISIGN and participants; rather, contractual obligations between CERTISIGN and participants are established by means of agreements with such participants.

This document is targeted at:

- CERTISIGN TRUST NETWORK PKI service providers who have to operate in terms of their own Certification Practices Statement (CPS) that complies with the requirements laid down by the CP
- CERTISIGN TRUST NETWORK certificate Subscribers who need to understand how they are authenticated and what their obligations are as CERTISIGN TRUST NETWORK subscribers and how they are protected under CERTISIGN TRUST NETWORK
- Relying parties who need to understand how much trust to place in a CERTISIGN TRUST NETWORK certificate, or a digital signature using that certificate

This CP conforms to the Internet Engineering Task Force (IETF) RFC 3647 for Certificate Policy and Certification Practice Statement construction.

CERTISIGN TRUST NETWORK conforms to the current version of (i) CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.6.3 (available at https://cabforum.org/baseline-requirements-documents/), (ii) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.8 (available at https://cabforum.org/extended-validation/) and (iii) CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates Certificates – version 1.4 (available at https://cabforum.org/ev-code-signing-certificate-guidelines/). In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

1.1 Overview

This CP is applicable to CERTISIGN ROOT CERTIFICATION AUTHORITY and Subordinates CAs:

- CERTISIGN SSL CERTIFICATION AUTHORITY
- CERTISIGN SSL EV CERTIFICATION AUTHORITY
- CERTISIGN CERTIFICATION AUTHORITY

CERTISIGN Subordinates CAs operate as CAs under CERTISIGN TRUST NETWORK CP, issuing end-user subscriber certificates as follow:

- CERTISIGN SSL CERTIFICATION AUTHORITY – issues SSL certificates under OV (Organization Validation) requirements;
- CERTISIGN SSL EV CERTIFICATION AUTHORITY – issues SSL certificates under EV (Extended Validation) requirements;
- CERTISIGN CERTIFICATION AUTHORITY– issues SSL certificates under DV (Domain Validation) requirements.

Registration Authorities (RAs) are entities that authenticate certificate requests under CERTISIGN TRUST NETWORK.

CERTISIGN and Affiliates act as RAs for certificates they issue. CERTISIGN and Affiliates also enter into contractual relationships with Enterprises who wish to manage their own certificate requests. These enterprise

customers act as RAs, authenticating certificate requests for themselves and their affiliated individuals. CERTISIGN or the Affiliate will then issue these authenticated certificate requests.

Depending on the type of certificate, Digital Certificates MAY be used by Subscribers to secure websites, digitally sign code or other content, digitally sign documents and/or e-mails. The person who ultimately receives a signed document or communication, or accesses a secured website is referred to as a relying party, i.e., he/she is relying on the certificate and has to make a decision on whether to trust it.

A Relying Party MUST rely on a certificate in terms of the relevant Relying Party Agreement listed in CERTISIGN TRUST NETWORK website.

1.2 Document Name and Identification

This document is CERTISIGN TRUST NETWORK CERTIFICATE POLICY (CP).

CERTISIGN TRUST NETWORK uses the OIDs below for its CAs:

Certificate Authority	OID
CERTISIGN ROOT CERTIFICATION AUTHORITY	1.3.6.1.4.1.30253.15
CERTISIGN SSL CERTIFICATION AUTHORITY	1.3.6.1.4.1.30253.16
CERTISIGN SSL EV CERTIFICATION AUTHORITY	1.3.6.1.4.1.30253.17
CERTISIGN CERTIFICATION AUTHORITY	1.3.6.1.4.1.30253.22

1.2.1 CABF Policy Identifiers

Not applicable.

1.2.2 Revision

Version	Description	Adopted
1.0	CERTISIGN TRUST NETWORK creation	09/13/2017
1.1	Adjust to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.5.4	10/10/2017
1.2	Adjust to EV Guidelines, v. 1.6.7 (itens 7.1.4.1.1; 7.1.4.2.3) and Appendix I	15/11/2017
1.3	Adjust to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.5.5 & 1.5.6	02/20/2018
1.4	✓ Adjust to Baseline Requirements for the Issuance and Management of PubliclyTrusted Certificates v. 1.5.7 & 1.5.8 ✓ Adjust to EV Guidelines, v. 1.6.8 ✓ Creation of SubCA: Certisign CA	06/06/2018
1.5	✓ Adjust to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.5.9 till 1.6.1 Adjust to Mozilla Requirements	12/18/2018
1.6	✓ Adjust to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 1.6.2 till 1.6.3 ✓ Adjust to Mozilla Requirements	02/06/2019

Table 1 - Revision

1.3 PKI Participants

1.3.1 Certification Authorities

Certification Authority (CA) is an organization that is responsible for the creation, issuance, revocation and management of Certificates.
The term applies equally to both Roots CAs and Subordinate CAs.

1.3.2 Registration Authorities

A Registration Authority is an entity that performs identification and authentication of certificate applicants for end-user certificates, initiates or passes along revocation requests for certificates for end-user certificates, and approves applications for renewal or re-keying certificates on behalf of a CERTISIGN TRUST NETWORK. CERTISIGN MAY act as an RA for certificates it issues.

Third parties, who enter into a contractual relationship with CERTISIGN, MAY operate their own RA and authorize the issuance of certificates by a CERTISIGN TRUST NETWORK. Third party RAs MUST abide by all the requirements of this CERTISIGN TRUST NETWORK CP, CERTISIGN TRUST NETWORK CP and the terms of their enterprise services agreement with CERTISIGN. RAs MAY, however implement more restrictive practices based on their internal requirements.

With the exception of sections 3.2.2.4 and 3.2.2.5, CERTISIGN MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

Before CERTISIGN authorizes a Delegated Third Party to perform a delegated function, CERTISIGN SHALL contractually require the Delegated Third Party to:
(1) Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
(2) Retain documentation in accordance with Section 5.5.2;
(3) Abide by the other provisions of these Requirements that are applicable to the delegated function; and
(4) Comply with (a) CERTISIGN CP or CPS or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

CERTISIGN MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization.

CERTISIGN SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:
1. The CA SHALL confirm that the requested Fully-Qualified Domain Name(s) are within the Enterprise RA's verified Domain Namespace.
2. If the certificate request includes a Subject name of a type other than a Fully-Qualified Domain Name, CERTISIGN SHALL confirm that the name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. For example, CERTISIGN SHALL NOT issue a Certificate containing the Subject name "XYZ Co." on the authority of Enterprise RA "ABC Co.", unless the two companies are affiliated (see Section 3.2) or "ABC Co." is the agent of "XYZ Co". This requirement applies regardless of whether the accompanying requested Subject FQDN falls within the Domain Namespace of ABC Co.'s Registered Domain Name.

CERTISIGN SHALL impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA.

1.3.3 Subscribers

Subscribers under CERTISIGN TRUST NETWORK include all end users (including entities) of certificates issued by CERTISIGN TRUST NETWORK. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers MAY be individuals, organizations, or infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

In some cases certificates are issued directly to individuals or entities for their own use. However, there commonly exist other situations where the party requiring a certificate is different from the subject to whom the credential applies. For example, an organization MAY require certificates for its employees to allow them to represent the organization in electronic transactions/business. In such situations the entity subscribing for the issuance of certificates (i.e. paying for them, either through subscription to a specific service, or as the issuer itself) is different from the entity which is the subject of the certificate (generally, the holder of the credential). Two different terms are used in this CP to distinguish between these two roles: "Subscriber", is the entity which contracts with CERTISIGN for the issuance of credentials and; "Subject", is the person to whom the credential is bound. The Subscriber bears ultimate responsibility for the use of the credential but the Subject is the individual that is authenticated when the credential is presented.

When 'Subject' is used, it is to indicate a distinction from the Subscriber. When "Subscriber" is used it MAY mean just the Subscriber as a distinct entity but MAY also use the term to embrace the two. The context of its use in this CP will invoke the correct understanding.

CAs are technically also subscribers of certificates within CERTISIGN TRUST NETWORK, either as a CA issuing a self-signed Certificate to itself, or as a CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CP, however, apply only to end-user Subscribers.

1.3.4 Relying Parties

A Relying Party is an individual or entity that acts in reliance of a certificate and/or a digital signature issued under CERTISIGN TRUST NETWORK. A Relying party MAY, or MAY NOT also be a Subscriber within CERTISIGN TRUST NETWORK.

1.3.5 Other Participants

Not applicable

1.4 Certificate Usage

1.4.1 Appropriate Certificate Usages

1.4.1.1 Certificates Issued to Individuals

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication).

1.4.1.2 Certificates Issued to Organizations

Organizational Certificates are issued to organizations after authentication that the Organization legally exists and that other Organization attributes included in the certificate (excluding non-verified subscriber information) are authenticated e.g. ownership of an Internet or e-mail domain.

1.4.1.3 EV Certificates

EV Certificates are intended for establishing Web-based data communication conduits via the TLS/SSL protocols and for verifying the authenticity of executable code.

The primary purposes of an EV Certificate are to:
i. Identify the legal entity that controls a Web site: Provide a reasonable assurance to the user of an Internet browser that the Web site the user is accessing is controlled by a specific legal entity identified in the EV Certificate by name, address of Place of Business, Jurisdiction of Incorporation or Registration and Registration Number or other disambiguating information; and
ii. Enable encrypted communications with a Web site: Facilitate the exchange of encryption keys in order to enable the encrypted communication of information over the Internet between the user of an Internet browser and a Web site.

The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:
i. Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
ii. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
iii. Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

EV Certificates focus only on the identity of the Subject named in the Certificate, and not on the behavior of the Subject.
As such, an EV Certificate is NOT intended to provide any assurances, or otherwise represent or warrant:
i. That the Subject named in the EV Certificate is actively engaged in doing business;
ii. That the Subject named in the EV Certificate complies with applicable laws;
iii. That the Subject named in the EV Certificate is trustworthy, honest, or reputable in its business dealings; or
iv. That it is "safe" to do business with the Subject named in the EV Certificate.

1.4.1.3.1 EV Certificates Applicants

CERTISIGN TRUST NETWORK MAY only issue EV Certificates to Applicants that meet these requirements:

- Private Organization Subjects

An Applicant qualifies as a Private Organization if:
(1) The entity's legal existence is created or recognized by a 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, registration number, etc.) or created or recognized by a Government Agency (e.g. under a charter, treaty, convention, or equivalent recognition instrument);
(2) The entity designated with the Incorporating or Registration Agency a Registered Agent, a Registered Office (as required under the laws of the Jurisdiction of Incorporation or Registration), or an equivalent facility;
(3) The entity is not designated on the records of the Incorporating or Registration Agency by labels such as "inactive," "invalid," "not current," or the equivalent;
(4) The entity has a verifiable physical existence and business presence;
(5) The entity's Jurisdiction of Incorporation, Registration, Charter, or License, and/or its Place of Business is not in any country where CERTISIGN TRUST NETWORK is prohibited from doing business or issuing a certificate by the laws of CERTISIGN TRUST NETWORK's jurisdiction; and
(6) The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CERTISIGN TRUST NETWORK's jurisdiction.

- Government Entity Subjects

An Applicant qualifies as a Government Entity if:
(1) The entity's legal existence was established by the political subdivision in which the entity operates;
(2) The entity is not in any country where CERTISIGN TRUST NETWORK is prohibited from doing business or issuing a certificate by the laws of CERTISIGN TRUST NETWORK's jurisdiction; and
(3) The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CERTISIGN TRUST NETWORK's jurisdiction.

- Business Entity Subjects

An Applicant qualifies as a Business Entity if:
(1) The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;
(2) The entity has a verifiable physical existence and business presence;
(3) At least one Principal Individual associated with the entity is identified and validated by CERTISIGN TRUST NETWORK;
(4) The identified Principal Individual attests to the representations made in the Subscriber Agreement;
(5) CERTISIGN TRUST NETWORK verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of CP Appendix C, item C;
(6) The entity and the identified Principal Individual associated with the entity are not located or residing in any country where CERTISIGN TRUST NETWORK is prohibited from doing business or issuing a certificate by the laws of CERTISIGN TRUST NETWORK's jurisdiction; and

(7) The entity and the identified Principal Individual associated with the entity are not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CERTISIGN TRUST NETWORK's jurisdiction.

- Non-Commercial Entity Subjects

An Applicant qualifies as a Non-Commercial Entity if:
(1) 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. CERTISIGN TRUST NETWORK/Browser Forum may publish a listing of Applicants who qualify as an International Organization for EV eligibility; and
(2) The Applicant is not headquartered in any country where CERTISIGN TRUST NETWORK is prohibited from doing business or issuing a certificate by the laws of CERTISIGN TRUST NETWORK's jurisdiction; and
(3) The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of CERTISIGN TRUST NETWORK's jurisdiction.

Subsidiary organizations or agencies of an entity that qualifies as a Non-Commercial Entity also qualifies for EV Certificates as a Non-Commercial Entity.

1.4.1.4 EV Code Signing Certificates

EV Code Signing Certificates and signatures are intended to be used to verify the identity of the certificate holder (Subscriber) and the integrity of its code. They provide assurance to a user or platform provider that code verified with the certificate has not been modified from its original form and is distributed by the legal entity identified in the EV Code Signing Certificate by name, Place of Business address, Jurisdiction of Incorporation or Registration, and other information. EV Code Signing Certificates may help to establish the legitimacy of signed code, help to maintain the trustworthiness of software platforms, help users to make informed software choices, and limit the spread of malware.

No particular software object is identified by an EV Code Signing Certificate, only its distributor is identified.
The secondary purposes of an EV Certificate are to help establish the legitimacy of a business claiming to operate a Web site or distribute executable code, and to provide a vehicle that can be used to assist in addressing problems related to phishing, malware, and other forms of online identity fraud. By providing more reliable third-party verified identity and address information regarding the business, EV Certificates may help to:
i. Make it more difficult to mount phishing and other online identity fraud attacks using Certificates;
ii. Assist companies that may be the target of phishing attacks or online identity fraud by providing them with a tool to better identify themselves to users; and
iii. Assist law enforcement organizations in their investigations of phishing and other online identity fraud, including where appropriate, contacting, investigating, or taking legal action against the Subject.

EV Code Signing Certificates focus only on assuring the identity of the Subscriber and that the signed code has not been modified from its original form. EV Code Signing Certificates are not intended to provide any other assurances, representations, or warranties. Specifically, EV Code Signing Certificates do not warrant that code is free from vulnerabilities, malware, bugs, or other problems. EV Code Signing Certificates do not warrant or represent that:
i. The Subject named in the EV Code Signing Certificate is actively engaged in doing business;
ii. The Subject named in the EV Code Signing Certificate complies with applicable laws;
iii. The Subject named in the EV Code Signing Certificate is trustworthy, honest, or reputable in its business dealings; or
v. It is "safe" to install code distributed by the Subject named in the EV Code Signing Certificate.

1.4.1.4.1 EV Code Signing Certificates Applicants

As described in section 1.4.1.3.1.

1.4.1.5 Assurance levels

Not applicable.

1.4.2 Prohibited Certificate Uses

Certificates SHALL be used only to the extent the use is consistent with applicable law, and in particular SHALL be used only to the extent permitted by applicable export or import laws.

CA Certificates MAY NOT be used for any functions except CA functions. In addition, end-user Subscriber Certificates SHALL NOT be used as CA Certificates.

1.5 Policy Administration

1.5.1 Organization Administering the Document

Certisign Certificadora Digital S.A.

Rua Bela Cintra, 904 – 11. Andar – São Paulo

Brasil

1.5.2 Contact Person

Normas e Compliance

Certisign Certificadora Digital S.A.

Rua Bela Cintra, 904 – 11. Andar – São Paulo

Brasil

(55 11 4501-2417)

normas@certisign.com.br

1.5.3 Person Determining CP Suitability for the Policy

CERTISIGN TRUST NETWORK Policy Management Department (PMD), named as "Normas e Compliance" determines the suitability and applicability of this CP.

1.5.4 CP Approval Procedure

Approval of this CP and subsequent amendments SHALL be made by the PMD. Amendments SHALL either be in the form of a document containing an amended form of the CP or an update notice. Amended versions or updates SHALL be linked to the Practices Updates and Notices section of the CERTISIGN Repository located at: http://ctn.certisign.com.br/ctn/certisign-trust-network.htm.

Updates supersede any designated or conflicting provisions of the referenced version of the CP.

1.5.5 EV Code Signing Policies

Each Issuer MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Code Signing Object practices, policies and procedures, such as this CP and its CPS:

i. Implement the requirements of these Guidelines as they are revised from time-to-time;
ii. Implement the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program or ETSI TS 102 042 V2.1.1; and
iii. Specify the Issuer's (and applicable Root CA's) entire root certificate hierarchy including all roots that its EV Code Signing Certificates depend on for proof of those EV Code Signing Certificates' authenticity.

With the exception of revocation checking for time-stamped and expired certificates, platforms are expected to validate signed code in accordance with RFC 5280. When a platform encounters a certificate that fails to validate due to revocation, the platform should reject the code. When a platform encounters a certificate that fails to validate for reasons other than revocation, the platform should treat the code as it would if it had been unsigned.

Ordinarily, a code signature created by a Subscriber may be considered valid for a period of up to thirty-nine months.
However, a code signature may be treated as valid for a period of up to 135 months by means of one of the following methods:
(A) Timestamp Method: In this method, the Subscriber signs the code, appends its EV Code Signing Certificate (whose expiration time is less than thirty-nine months in the future) and submits it to an EV Timestamp Authority to be time-stamped. The resulting package can be considered valid up to the expiration time of the timestamp certificate (which may be up to 135 months in the future).
(B) Signing Authority Method: In this method, the Subscriber submits the code, or a digest of the code, to an EV Signing Authority for signature. The resulting signature is valid up to the expiration time of the Signing Authority certificate (which may be up to 135 months in the future).

1.6 Definitions and Acronyms

1.6.1 Definitons
See Appendix A for a table of Definitions.

1.6.2 Acronyms
See Appendix A for a table of Acronyms.

1.6.3. References
See Appendix B for a list of References.

1.6.4. Conventions
The key words “MUST”, “MUST NOT”, "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in these Requirements SHALL be interpreted in accordance with RFC 2119.

2. Publication and Repository Responsibilities

2.1 Repositories
CERTISIGN and Affiliates are responsible for maintaining a publicly accessible online repository, as well as revocation information concerning Certificates they issue.

2.2 Publication of Information
CERTISIGN and Affiliates maintain a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. Any exception to this SHALL be approved by the PMD on a case by case basis and MUST be documented in the appropriate CP. CERTISIGN and Affiliates provide Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP (Online Certificate Status Protocol) is available, how to find the right OCSP responder.

CERTISIGN publishs the Certificates it issues on behalf of its own CAs, and the CAs in their Sub-domain. Upon revocation of an end-user Subscriber’s Certificate, CERTISIGN publishs notice of such revocation in the repository. In addition, CERTISIGN issues Certificate Revocation Lists (CRLs) and, if available, provide OCSP services (Online Certificate Status Protocol) for its own CAs and the CAs within their respective Sub-domains.

CERTISIGN will at all times publish a current version of the following documents in its repositories:
- This CERTISIGN TRUST NETWORK CP,
- CERTISIGN TRUST NETWORK CPS,
- Subscriber Agreements,
- Relying Party Agreements

CERTISIGN garantees that its repository is accessible online on a 24x7 basis and that its CP and/or CPS disclose its CERTISIGN TRUST NETWORK business practices as required by WebTrust for CAs and ETSI TS 102 042 and ETSI EN 319 411-1.

2.3 Time or Frequency of Publication

CERTISIGN TRUST NETWORK develops, implements, enforces, and at least annually updates this CP and its CPS.
Updates to Subscriber Agreements and Relying Party Agreements are published as necessary.
Certificates are published upon issuance.
Certificate status information is published in accordance with the provisions of this CP.

2.4 Access Controls on Repositories

CERTISIGN and Affiliates SHALL NOT intentionally use technical means of limiting access to this CP, their CPS, Certificates, Certificate status information, or CRLs. CERTISIGN and Affiliates SHALL, however, require persons to agree to a Relying Party Agreement or CRL Usage Agreement as a condition to accessing Certificates, Certificate status information or CRLs. CERTISIGN and Affiliates SHALL implement controls to prevent unauthorized persons from adding, deleting, or modifying repository entries.

3. Identification and Authentication

3.1 Naming

Unless where indicated otherwise in this CP, its CPS, names appearing in Certificates issued under CERTISIGN TRUST NETWORK are authenticated.

3.1.1 Type of Names

CERTISIGN TRUST NETWORK CA Certificates contains:

- an X.501 Distinguished Name (DN) in the Subject name field and in the Issuer Name field,
- MAY contain multiple OU attributes,
- its DN is formed as below:

Attribute	Value
Country (C) =	BR
Organization (O) =	Certisign Certificadora Digital S.A.
Common Name (CN) =	<Certificate Authority Name>

Table 2- Distinguished Name Attributes in CA Certificates

End-user Subscriber Certificates contains:

- an X.501 Distinguished Name (DN) in the Subject name field and in the Issuer Name field,
- MAY contain multiple OU attributes,
- its DN is formed as below:

Attribute	Value
Country (C) =	2-letter ISO country code or not used.
Organization (O) =	<organization name>
Organizational Unit (OU) =	<organization unit>
State or Province (ST) =	Indicates the Subscriber's State or Province (OPTIONAL)
Locality (L) =	Indicates the Subscriber's Locality (Locality is not a REQUIRED field in certificates issued to individuals). (Optional)
Common Name (CN) =	. OCSP Responder Name (for OCSP Responder Certificates) . Domain name (for web server Certificates) . Organization name (for code/object signing Certificates or organization Certificates) . Person's name (for individual Certificates or code-signing certificates issued to individuals).

Table 3 - Distinguished Name Attributes in End User Subscriber Certificates

3.1.1.1 CABF Naming Requirements

Domain validated and organization validated SSL Certificates conform to the CA / Browser Forum Baseline requirements.

Issuer Fields

The following naming attributes SHALL be used to populate the Issuer in Certificates issued under this CPS:

Issuer CountryName (REQUIRED)
The countryName (C=) component is REQUIRED and contains the two-letter ISO 3166-1 country code for the country in which the issuer's place of business is located.

Issuer organizationName (REQUIRED)
The organizationName (O=) field is REQUIRED and contains the Issuer organization name (or abbreviation thereof), trademark, or other meaningful identifier for the CA, that accurately identifies the CA. The field MUST NOT contain a generic designation such as "Root" or "CA1".

Issuer commonName (OPTIONAL)
If the Issuer commonName (CN=) field is present, it MUST contain a name that accurately identifies the Issuing CA.

Subject Fields

The following naming attributes SHALL be used to populate the Subject in Certificates issued under this CPS:

subjectAlternativeName (REQUIRED)
- The subjectAlternativeName extension is REQUIRED and contains at least one entry.

- In SSL Certificates, each entry is either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server.

- CERTISIGN TRUST NETWORK confirms that the Applicant controls the Fully-Qualified Domain Name (FQDN) or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.

- Wildcard FQDNs are permitted.

- Issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Server Name is NOT permitted.

CountryName (OPTIONAL)
- If present, the countryName (C=) component SHALL be the two-letter ISO 3166-1 country code.

- If present, CERTISIGN TRUST NETWORK SHALL verify the country associated with the Subject in accordance with CP section 3.2.2.

OrganizationName (OPTIONAL)
- If the organizationName (O=) field is present, the field contains the Subject's name or DBA and the REQUIRED address fields contain a location of the Subject as verified in accordance with CP section 3.2.2.

- If the Subject is a natural person, because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey the Subject's name or DBA (see CP section 3.2.2.1).

- If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA SHALL document the discrepancy and SHALL use locally accepted abbreviations when abbreviating the organization name (e.g., if the official record shows "Company Name Incorporated", the CA

MAY include "Company Name, Inc."). The organizationName field MAY include a verified DBA or tradename of the Subject.

- If organizationName is present, then localityName, stateOrProvinceName (where applicable), and countryName SHALL also be REQUIRED and streetAddress and postalCode are OPTIONAL. If organizationName is absent, then the Certificate SHALL NOT contain a streetAddress, localityName, stateOrProvinceName or postalCode attribute. The CA MAY include the Subject's countryName field without including other Subject Identity Information pursuant to countryName requirements above.

OrganizationalUnitName (OPTIONAL)

- The OrganizationalUnitName (OU=) component, when present, MAY contain information that has not been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, SHALL NOT be used.

- The CA implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with CP section 3.2.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with CP section 3.2.2.

- When an OU value is submitted in a Request, the value is subjected to a search of various high risk lists as per CP section 3.2.2.1, High Risk Requests. If a match is found, the value is reviewed by the RA to ensure that the value is accurate and not misleading. If the OU value identifies the name of a legal entity, the value is verified in accordance with CP section 3.2.2.1, Verification of Subject Identity comprised of Country Name and Other Identity Information.

commonName (OPTIONAL)

The commonName (CN=) component is deprecated (discouraged, but not prohibited). If present, commonName MUST contains a single IP address or FQDN that is also one of the values contained in the Certificate's subjectAlternativeName extension.

domainComponent (OPTIONAL)

The domainComponent (dc=) component is OPTIONAL. If present, domainComponent contains all components of the subject's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.

Other Subject Attributes

- Optional attributes, when present in the subject field, MUST contain information that has been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, SHALL NOT be used.

- CERTISIGN TRUST NETWORK SHALL NOT include Fully-Qualified Domain Names in Subject attributes except as specified for subjectAlternativeName and CommonName above.

3.1.1.1.1 CABF Naming Requirements for EV

Issuer Information listed in an EV Certificate MUST comply with Section 7.1.4.1 of its CP.

3.1.2 Need for Names to be Meaningful

CERTISIGN TRUST NETWORK CA Certificates and End-user Subscriber contains names with commonly understood semantics permitting the determination of the identity of the CA that is the Subject of the Certificate.

End-user Subscriber Certificates shall contain names with commonly understood semantics permitting the determination of the identity of the individual or organization that is the Subject of the Certificate.

3.1.3 Anonymity or Pseudonymity of Subscribers
Subscribers are not permitted to use pseudonyms (names other than a Subscriber's true personal or organizational name). Each request for anonymity in a certificate will be evaluated on its merits by the PMD and, if allowed the certificate will indicate that identity has been authenticated but is protected.

3.1.4 Rules for Interpreting Various Name Forms
No stipulation.

3.1.5 Uniqueness of Names
CERTISIGN ensures that Subject Distinguished Name (DN) of the Subscriber is unique within the domain of a specific CA through automated components of the Subscriber enrollment process.

It is possible for a Subscriber to have two or more certificates with the same Subject Distinguished Name (DN).

3.1.6 Recognition, Authentication, and Role of Trademarks
Certificate Applicants SHALL NOT use names in their Certificate Applications that infringe upon the Intellectual Property Rights of others. CERTISIGN SHALL be REQUIRED to determine whether a Certificate Applicant has Intellectual Property Rights in the name appearing in a Certificate Application or to arbitrate, mediate, or otherwise resolve any dispute concerning the ownership of any domain name, trade name, trademark, or service mark, and CERTISIGN SHALL be entitled, without liability to any Certificate Applicant, to reject or suspend any Certificate Application because of such dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key
The certificate applicant MUST demonstrate that it rightfully holds the private key corresponding to the public key to be listed in the Certificate.

The method to prove possession of a private key SHALL be PKCS #10, another cryptographically equivalent demonstration, or another CERTISIGN-approved method. This requirement does not apply where a key pair is generated by a CA on behalf of a Subscriber[1].

3.2.1.1. CABF Verification Requirements for EV
See Appendix C: EV Verification Requirements.

3.2.2 Authentication of Organization and Domain Identity
Whenever a certificate contains an *organization name*, the identity of the organization and other enrollment information provided by Certificate Applicants (except for Non-verified Subscriber Information) is confirmed in accordance with the procedures set forth in this CP and/or CERTISIGN's internal documents.

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the *countryName* field, then CERTISIGN SHALL verify the country associated with the Subject using a verification process meeting the requirements of Section 3.2.2.3 and that is described in this this CP and/or CERTISIGN's internal documents. If the Applicant requests a Certificate that will contain the *countryName* field and other Subject Identity Information, CERTISIGN 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 this Section 3.2.2.1 and that is described in this CP and/or CERTISIGN's internal documents..

CERTISIGN SHALL inspect any document relied upon under this Section for alteration or falsification.

[1]for example where pre-generated keys are placed on smart cards

3.2.2.1. Identity

CERTISIGN or an Affiliate SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. determine that the organization exists by using at least one third party identity proofing service or database, or alternatively, organizational documentation issued by or filed with the applicable government agency or recognized authority that confirms the existence of the organization,
2. confirm by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so[2].
3. A site visit by CERTISIGN TRUST NETWORK or a third party who is acting as an agent for the CA
4. An Attestation Letter
5. When a certificate includes the name of an individual as an authorized representative of the Organization, the employment of that individual and his/her authority to act on behalf of the Organization shall also be confirmed.
6. Where a domain name or e-mail address is included in the certificate CERTISIGN authenticates the Organization's right to use that domain name either as a fully qualified Domain name or an e-mail domain.

CERTISIGN TRUST NETWORK MAY use the same documentation or communication described above to verify both the Applicant's identity and address.

Alternatively, CERTISIGN TRUST NETWORK MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that CERTISIGN TRUST NETWORK determines to be reliable.

3.2.2.2. DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, CERTISIGN TRUST NETWORK SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:
1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames;
4. An Attestation Letter accompanied by documentary support; or
5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that CERTISIGN TRUST NETWORK determines to be reliable.

3.2.2.3. Verification of Country

If the subject:countryName field is present, then CERTISIGN TRUST NETWORK SHALL verify the country associated with the Subject using one of the following:
(a) the IP Address range assignment by country for either
    (i) the web site's IP address, as indicated by the DNS record for the web site or
    (ii) the Applicant's IP address;
(b) the ccTLD of the requested Domain Name;
(c) information provided by the Domain Name Registrar; or
(d) a method identified in Section 3.2.2.1.

CERTISIGN TRUST NETWORK SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4. Validation of Domain Authorization or Control

This section defines the permitted processes and procedures for validating the Applicant's ownership or control of the domain.

2 This option isn´t allowed to issue under CA/Browser Forum - Baseline Requirements

CERTISIGN TRUST NETWORK SHALL confirm that prior to issuance, CERTISIGN TRUST NETWORK has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed below. Completed validations of Applicant authority may be valid for the issuance of multiple Certificates over time. In all cases, the validation must have been initiated within the time period specified in the relevant requirement prior to Certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's Parent Company, Subsidiary Company, or Affiliate.
CERTISIGN TRUST NETWORK SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.
Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

3.2.2.4.1 Validating the Applicant as a Domain Contact

1. CERTISIGN TRUST NETWORK authenticates the Applicant's identity under Section 3.2.2.1 and the authority of the Applicant Representative under Section 3.2.5, or
2. CERTISIGN TRUST NETWORK authenticates the Applicant's identity under EV Guidelines Section 11.2 (transcripted at Appendix C – item 2) and the agency of the Certificate Approver under EV Guidelines Section 11.8 (transcripted at Appendix C – item 8); or
3. CERTISIGN TRUST NETWORK is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

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

For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.
Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.
CERTISIGN TRUST NETWORK MAY send the email, fax, SMS, or postal mail 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, fax, SMS, or postal mail. The Random Value SHALL be unique in each email, fax, SMS, or postal mail.
CERTISIGN TRUST NETWORK MAY resend the email, fax, SMS, or postal mail 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. The CPS MAY specify a shorter validity period for Random Values, in which case CERTISIGN TRUST NETWORK MUST follow its CPS.

Note: (i) Once the FQDN has been validated using this method, CERTISIGN TRUST NETWORK MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN. (ii)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 FQDN by calling the Domain Name Registrant's phone number and obtaining a response confirming the Applicant's request for validation of the FQDN. CERTISIGN TRUST NETWORK MUST place the call to a phone number identified by the Domain Name Registrar as the Domain Contact.
Each phone call SHALL be made to a single number and MAY confirm control of multiple FQDNs, provided that the phone number is identified by the Domain Registrar as a valid contact method for every Base Domain Name being verified using the phone call.

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

3.2.2.4.4 Constructed Email to Domain Contact

Confirm the Applicant's control over the 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 recipient SHALL remain unchanged.
The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

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

3.2.2.4.5 Domain Authorization Document

Confirming the Applicant's control over the FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document MUST substantiate that the communication came from the Domain Contact.

CERTISIGN TRUST NETWORK MUST verify that the Domain Authorization Document was either

(i) dated on or after the date of the domain validation request or
(ii) that the WHOIS data has not materially changed since a previously provided Domain Authorization Document for the Domain Name Space.

For certificates issued on or after August 1, 2018, this method SHALL NOT be used for validation, and completed validations using this method SHALL NOT be used for the issuance of certificates.

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the FQDN by confirming one of the following 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 by CERTISIGN TRUST NETWORK via HTTP/HTTPS over an Authorized Port:
1. The presence of Required Website Content contained in the content of a file. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Random Value contained in the content of a file where the Request Token or Random Value MUST NOT appear in the request.
If a Random Value is used, CERTISIGN TRUST NETWORK SHALL provide a Random Value unique to the certificate request and SHALL not use the Random Value after the longer of (i) 30 days or (ii) if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate).

Note: Examples of Request Tokens include, but are not limited to:
(i) a hash of the public key;
(ii) a hash of the Subject Public Key Info [X.509]; and
(iii) a hash of a PKCS#10 CSR.

A Request Token may also be concatenated with a timestamp or other data.
If CERTISIGN TRUST NETWORK wanted to always use a hash of a PKCS#10 CSR as a Request Token and did not want to incorporate a timestamp and did want to allow certificate key re-use then the applicant might use the

challenge password in the creation of a CSR with OpenSSL to ensure uniqueness even if the subject and key are identical between subsequent requests.
This simplistic shell command produces a Request Token which has a timestamp and a hash of a CSR.
E.g. echo date -u +%Y%m%d%H%M sha256sum <r2.csr | sed "s/[-]//g"

The script outputs: 201602251811c9c863405fe7675a3988b97664ea6baf442019e4e52fa335f406f7c5f26cf14f

CERTISIGN TRUST NETWORK should define in its CPS the format of Request Tokens it accepts.

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

3.2.2.4.7 DNS Change

Confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, 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.

If a Random Value is used, CERTISIGN TRUST NETWORK 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.

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

3.2.2.4.8 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN in accordance with section 3.2.2.5.

Note: (i) Once the FQDN has been validated using this method, CERTISIGN TRUST NETWORK MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless CERTISIGN TRUST NETWORK performs a separate validation for that FQDN using an authorized method. (ii) This method is NOT suitable for validating Wildcard Domain Names.

3.2.2.4.9 Test Certificate for EV Certificates

Confirming the Applicant's control over the FQDN by confirming the presence of a non-expired Test Certificate issued by CERTISIGN TRUST NETWORK on the Authorization Domain Name and which is accessible by CERTISIGN TRUST NETWORK via TLS over an Authorized Port for the purpose of issuing a Certificate with the same Public Key as in the Test Certificate.

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

3.2.2.4.10. TLS Using a Random Number

Confirming the Applicant's control over the requested FQDN by confirming the presence of a Random Value within a Certificate on the Authorization Domain Name which is accessible by CERTISIGN TRUST NETWORK TLS over an Authorized Port.

3.2.2.4.11 Any Other Method

This method has been retired and MUST NOT be used.

3.2.2.4.12 Validating Applicant as a Domain Contact

Confirming the Applicant's control over the FQDN by validating the Applicant is the Domain Contact. This method may only be used if CERTISIGN SSL EV CERTIFICATION AUTHORITY is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

Note: Once the FQDN has been validated using this method, CERTISIGN SSL EV CERTIFICATION AUTHORITY 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.

3.2.2.4.13 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. The same email MAY be sent to multiple recipients as long as all recipients are DNS CAA Email Contacts for each Authorization Domain Name being validated.

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 recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA 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 for the Authorization Domain Name selected to validate the FQDN.

Each email MAY confirm control of multiple FQDNs, provided that each email address is DNS TXT Record Email Contact for each Authorization Domain Name being validated. The same email MAY be sent to multiple recipients as long as all recipients are DNS TXT Record Email Contacts for each Authorization Domain Name being validated.

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 recipient(s) SHALL remain unchanged. The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Note: Once the FQDN has been validated using this method, the CA 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

For each IP Address listed in a Certificate, CERTISIGN TRUST NETWORK SHALL confirm that, as of the date the Certificate was issued, the Applicant has control over the IP Address by:
1. Having the Applicant demonstrate practical control over the IP Address by making an agreed-upon change to information found on an online Web page identified by a uniform resource identifier containing the IP Address;
2. Obtaining documentation of IP address assignment from the Internet Assigned Numbers Authority (IANA) or a Regional Internet Registry (RIPE, APNIC, ARIN, AfriNIC, LACNIC);
3. Performing a reverse-IP address lookup and then verifying control over the resulting Domain Name under Section 3.2.2.4; or
4. Using any other method of confirmation, provided that CERTISIGN TRUST NETWORK maintains documented evidence that the method of confirmation establishes that the Applicant has control over the IP Address to at least the same level of assurance as the methods previously described.

Note: IPAddresses MAY be listed in Subscriber Certificates using IPAddress in the subjectAltName extension or in Subordinate CA Certificates via IPAddress in permittedSubtrees within the Name Constraints extension.

3.2.2.6. Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, CERTISIGN TRUST NETWORK or its Affiliates MUST establish and follow a documented 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".[3]

If a wildcard would fall within the label immediately to the left of a registry-controlled or public sufix[4], CERTISIGN TRUST NETWORK MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace e.g. CERTISIGN TRUST NETWORK MUST NOT issue "*.co.uk" or "*.local", but MAY issue "*.example.com" to Example Co.

3.2.2.7. Data Source Accuracy

Prior to using any data source as a Reliable Data Source, CERTISIGN TRUST NETWORK SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. CERTISIGN TRUST NETWORK SHOULD consider the following during its evaluation:
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.

Databases maintained by CERTISIGN TRUST NETWORK , its owner, or its affiliated companies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.8. CAA Records

Effective as of 8 September 2017, as part of SSL issuance process under CA/Browser Forum - Baseline Requirements, CERTISIGN TRUST NETWORK MUST check for CAA records and follow the processing instructions for any records found, for each dNSName in the subjectAltName extension of the certificate to be issued, as specified in RFC 6844 as amended by Errata 5065 (Appendix H). If CERTISIGN TRUST NETWORK issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

The Certification Authority CAA identifying domains for CAs within CTN operational control are "certisign.com", "certisign.com.br" and any domain containing those identifying domains as suffixes (e.g. example.certisign.com).

This stipulation does not prevent CERTISIGN TRUST NETWORK from checking CAA records at any other time. When processing CAA records, CERTISIGN TRUST NETWORK MUST process the issue, issuewild, and iodef property tags as specified in RFC 6844, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but MUST NOT conflict with or supersede the mandatory property tags set out in this document. CERTISIGN TRUST NETWORK MUST respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set.
RFC 6844 requires that CERTISIGN TRUST NETWORK MUST NOT issue a certificate unless either
(1) the certificate request is consistent with the applicable CAA Resource Record set or

---

[3] See RFC 6454 Section 8.2 for further explanation

[4] Determination of what is "registry-controlled" versus the registerable portion of a Country Code Top-Level Domain Namespace is not standardized at the time of writing and is not a property of the DNS itself. Current best practice is to consult a "public suffix list" such as http://publicsuffix.org/ (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

(2) an exception specified in CP or CPS applies.

CERTISIGN TRUST NETWORK MUST NOT rely on any exceptions specified in their CP or CPS unless they are one of the following:
• CAA checking is OPTIONAL for certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
• CAA checking is OPTIONAL for certificates issued by a Technically Constrained Subordinate CA Certificate as set out in section 7.1.5, where the lack of CAA checking is an explicit contractual provision in the contract with the Applicant.
• CAA checking is OPTIONAL if CERTISIGN TRUST NETWORK or its Affiliates is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CERTISIGN TRUST NETWORK is permitted to treat a record lookup failure as permission to issue if:
• the failure is outside the it's infrastructure;
• the lookup has been retried at least once; and
• the domain's zone does not have a DNSSEC validation chain to the ICANN root.

CERTISIGN TRUST NETWORK MUST document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback to the CAB Forum on the circumstances, and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present.

CERTISIGN TRUST NETWORK is not expected to support URL schemes in the iodef record other than *mailto:* or *https:*.

As effective on April, 4h, 2018 certificates will only be considered "trusted" by Chrome if aligned with Certificate Transparence Requirements.

3.2.2.9 CABF Verification Requirements for Organization Applicants

Validation procedures for issuing Certificates containing internationalized domain names (IDNs) SHALL be documented in CERTISIGN TRUST NETWORK CPS. Procedures that validate the owner of a domain, attending Mozilla requirements, SHALL prevent against homographic spoofing of IDNs and SHALL fully comply with the CA/Browser Forum requirements for IDN certificates.

CERTISIGN employs a process that searches various 'whois' services to find the owner of a particular domain. A search failure result is flagged for manual review and the RA manually rejects the Certificate Request. Additionally, the RA rejects any domain name that visually appears to be made up of multiple scripts within one hostname label.

3.2.3 Authentication of Individual Identity

If an Applicant subject to this Section is a natural person, then CERTISIGN TRUST NETWORK SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

The agent SHALL check the identity of the Certificate Applicant against a well-recognized form of government-issued photographic identification, such as a passport, driver's license, military ID, national ID, or equivalent document type.

The agent listed above SHALL verify the Applicant's address using a form of identification that CERTISIGN TRUST NETWORK determines to be reliable, such as a government ID, utility bill, or bank or credit card statement . CERTISIGN TRUST NETWORK MAY rely on the same government-issued ID that was used to verify the Applicant's name.

CERTISIGN TRUST NETWORK SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

3.2.4 Non-Verified Subscriber information

Non-verified subscriber information includes:

- Organization Unit (OU) with certain exceptions[5]
- Any other information designated as non-verified in its CP.

3.2.5 Validation of Authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, CERTISIGN TRUST NETWORK SHALL use a Reliable Method of Communication to verify the authenticity of the Applicant Representative's certificate request.

CERTISIGN TRUST NETWORK MAY use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication.

Provided that CERTISIGN TRUST NETWORK uses a Reliable Method of Communication, CERTISIGN TRUST NETWORK MAY establish the authenticity of the certificate request directly with the Applicant Representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that CERTISIGN TRUST NETWORK deems appropriate.

3.2.5.1. CABF Verification Requirements for SSL Certificates

In SSL certificate issuance process under CA/Browser Forum - Baseline Requirements, CERTISIGN TRUST NETWORK SHALL establish a process that allows an Applicant to specify the individuals who MAY request Certificates. If an Applicant specifies, in writing, the individuals who MAY request a Certificate, then CERTISIGN TRUST NETWORK SHALL NOT accept any certificate requests that are outside this specification. CERTISIGN TRUST NETWORK SHALL provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation

CERTISIGN MAY provide interoperation services that allow any CA to be able to interoperate with CERTISIGN TRUST NETWORK by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with CERTISIGN TRUST NETWORK CP as supplemented by additional policies when required.

CERTISIGN SHALL only allow interoperation with CERTISIGN TRUST NETWORK of any CA in circumstances where CERTISIGN TRUST NETWORK SHALL at a minimum:

- Enters into a contractual agreement with CERTISIGN or an Affiliate
- Operates under a CPS that meets CERTISIGN TRUST NETWORK requirements for the type of certificates it will issue
- Passes a compliance assessment before being allowed to interoperate
- Passes an annual compliance assessment for ongoing eligibility to interoperate.

CERTISIGN TRUST NETWORK SHALL disclose all Cross Certificates that identify CERTISIGN TRUST NETWORK as the Subject, provided that CERTISIGN TRUST NETWORK arranged for or accepted the establishment of the trust relationship (i.e. the Cross Certificate at issue).

3.3 Identification and Authentication for Re-key Requests

Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to obtain a new certificate to maintain continuity of Certificate usage. CERTISIGN TRUST NETWORK and RAs generally require that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey"). However, in certain cases (i.e., for web server certificates) Subscribers MAY request a new certificate for an existing key pair (technically defined as "renewal").

[5] Domain-validated and organization-validated certificates MAY contain Organizational Unit values that are validated.

Generally speaking, both "Rekey" and "Renewal" are commonly described as "Certificate Renewal", focusing on the fact that the old Certificate is being replaced with a new Certificate and not emphasizing whether or not a new key pair is generated. When there is a distinction between "rekey" and "renewal", it will be pointed.

3.3.1 Identification and Authentication for Routine Re-key

As defined at Section 4.2.1.

Re-key procedures ensure that the person or organization seeking to rekey an end-user Subscriber Certificate is in fact the Subscriber of the Certificate.

One acceptable procedure is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, and the enrollment information (including Corporate and Technical contact information) has not changed, a renewal Certificate is automatically issued. As an alternative to using a challenge phrase (or equivalent) CERTISIGN may send an e-mail message to the e-mail address associated with the verified corporate contact for the certificate being renewed, requesting confirmation of the Certificate renewal order and authorization to issue the Certificate. Upon receipt of confirmation authorizing issuance of the Certificate, CERTISIGN will issue the Certificate if the enrollment information (including Corporate and Technical contact information) has not changed[6].

After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, CERTISIGN or the RA reconfirms the identity of the Subscriber in accordance with the identification and authentication requirements of an original Certificate Application.

Rekey after 30-days from expiration of the Certificate are re-authenticated as an original Certificate Application and are not automatically issued.

3.3.2 Identification and Authentication for Re-key After Revocation

Re-key/renewal after revocation is not permitted.

3.4 Identification and Authentication for Revocation Request

Revocation procedures ensure prior to any revocation of any Certificate that the revocation has in fact been requested by the Certificate's Subscriber, the entity that approved the Certificate Application, or the applicable CA.

Acceptable procedures for authenticating the revocation requests of a Subscriber include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or the equivalent thereof), and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent thereof) on record. (Note that this option MAY NOT be available to all customers.)
- Receiving a message from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked,
- Communication with the Subscriber providing reasonable assurances that the person or organization requesting revocation is, in fact the Subscriber. Such communication, depending on the circumstances, MAY include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

CA/RA Administrators are entitled to request the revocation of end-user Subscriber Certificates within the CA's/RA's Sub domain. CERTISIGN and Affiliates authenticate the identity of Administrators via client authentication before permitting them to perform revocation functions, or another CERTISIGN TRUST NETWORK-approved procedure.

[6] If contact information has changed via an approved formal contact change procedure the certificate shall still qualify for automated renewal.

The requests to revoke a CA Certificate SHALL be authenticated by the requesting entity's Superior entity to ensure that the revocation has in fact been requested by the CA.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who Can Submit a Certificate Application?

Below is a list of people who MAY submit certificate applications:

- Any individual who is the subject of the certificate,
- Any authorized representative of an Organization or entity,
- Any authorized representative of a CA,
- Any authorized representative of an RA.

4.1.1.1. CABF Certificate Application Requirements for SSL Certificates

In accordance with CPS Section 5.5.2, CERTISIGN TRUST NETWORK SHALL maintain an internal database of all previously revoked SSL Certificates and previously rejected certificate requests due to suspected phishing or other fraudulent usage or concerns. CERTISIGN TRUST NETWORK SHALL use this information to identify subsequent suspicious certificate requests.

4.1.2 Enrollment Process and Responsibilities

4.1.2.1 End-User Certificate Subscribers

All end-user Certificate Subscribers SHALL manifest assent to the relevant Subscriber Agreement (which MAY be electronic) that contains representations and warranties described in Section 9.6.3 and undergo an enrollment process consisting of:

- completing a Certificate Application, which MAY be electronic and providing true and correct information,
- generating, or arranging to have generated, a key pair,
- delivering his, her, or its public key, directly or through an RA, to CA,
- demonstrating possession and/or exclusive control of the private key corresponding to the public key delivered to the CA.

4.1.2.2 CABF Certificate Application Requirements

4.1.2.2.1 SSL Certificates

Prior to the issuance of a SSL Certificate, CERTISIGN TRUST NETWORK SHALL obtain from the Applicant a certificate request in a form prescribed by CERTISIGN TRUST NETWORK and that complies with these Requirements. One SSL certificate request MAY suffice for multiple Certificates to be issued to the same Applicant, subject to the aging and updating requirement in Section 3.3.1, provided that each SSL Certificate is supported by a valid, current certificate request signed by the appropriate Applicant Representative on behalf of the Applicant. The certificate request MAY be made, submitted and/or signed electronically.

The SSL certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

Request and Certification

The certificate request MUST contain a request from, or on behalf of, the Applicant for the issuance of a Certificate, and a certification by, or on behalf of, the Applicant that all of the information contained therein is correct.

Information Requirements
The certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for the CA to obtain from the Applicant in order to comply with these Requirements and the CA's Certificate Policy and/or Certification Practice Statement. In cases where the certificate request does not contain all the necessary information about the Applicant, the Certisign CA SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant.
Applicant information MUST include, but not be limited to, at least one FQDN to be included in the Certificate's *SubjectAltName*extension.

Subscriber Private Key
Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key.
If the CA or any of its designated RAs generated the Private Key on behalf of the Subscriber, then the CA SHALL encrypt the Private Key for transport to the Subscriber.
If the CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

Subscriber and Agreement
Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, the Applicant's agreement to the Subscriber Agreement with the CA.
The CA SHALL implement a process to ensure that each Subscriber Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request.
CERTISIGN TRUST NETWORK uses an electronic or "click-through" Agreement; such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber Agreement.

4.1.2.2.1 EV and EV CodeSigning Certificates

Role Requirements
The following Applicant roles are required for the issuance of an EV Certificate.
. Certificate Requester: The EV Certificate Request MUST 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 agentwho has express authority to represent the Applicant, or a third party (such as an ISP or hosting company) that completes and submits an EV Certificate Request on behalf of the Applicant.

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

. Contract Signer: A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

. Applicant Representative: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any of these roles.

EV Certificate Request Requirements
The Certificate Request requirements in Section 4.1.2 apply equally to EV Certificates subject to the additional more stringent ageing and updating requirement of Appendix C, item 14 of this CP.

Requirements for Subscriber Agreement and Terms of Use
Section 9.6.3 applies equally to EV Certificates. In cases where the Certificate Request does not contain all necessary information about the Applicant, the CA MUST additionally confirm the data with the Certificate Approver or Contract Signer rather than the Certificate Requester.

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions
An RA SHALL perform identification and authentication of all required Subscriber information in terms of Section 3.2.

The SSL certificate request MAY include all factual information about the Applicant to be included in the Certificate, and such additional information as is necessary for CERTISIGN TRUST NETWORK to obtain from the Applicant in order to comply with these Requirements and the CA's CP and/or CPS. In cases where the certificate request does not contain all the necessary information about the Applicant, CERTISIGN TRUST NETWORK SHALL obtain the remaining information from the Applicant or, having obtained it from a reliable, independent, third-party data source, confirm it with the Applicant. CERTISIGN TRUST NETWORK establishs and follows a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

Applicant information MUST include, but not be limited to, at least one FQDN or IP address to be included in the Certificate's SubjectAltName extension.

4.2.1.1. CABF Requirements for SSL Certificates
Section 6.3.2 limits the validity period of Subscriber Certificates. CERTISIGN TRUST NETWORK MAY use the documents and data provided in Section 3.2 to verify certificate information, or may reuse previous validations themselves, provided that:

(1) Prior to March 1, 2018, CERTISIGN TRUST NETWORK obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 39 months prior to issuing the Certificate; and

(2) On or after March 1, 2018, CERTISIGN TRUST NETWORK obtained the data or document from a source specified under Section 3.2 or completed the validation itself no more than 825 days prior to issuing the Certificate.

In no case may a prior validation be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

After the change to any validation method specified in the Baseline Requirements or EV Guidelines, CERTISIGN TRUST NETWORK may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this CP unless otherwise specifically provided in a ballot.

Validations completed using methods specified in Section 3.2.2.4.1 or Section 3.2.2.4.5 SHALL NOT be re-used on or after August 1, 2018.

CERTISIGN TRUST NETWORK SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under these Requirements.

If a Delegated Third Party fulfills any of the CA's obligations under this section, CERTISIGN TRUST NETWORK SHALL verify that the process used by the Delegated Third Party to identify and further verify High Risk Certificate Requests provides at least the same level of assurance as the CA's own processes.

4.2.2 Approval or Rejection of Certificate Applications

An RA will approve an application for a certificate if the following criteria are met:

- Successful identification and authentication of all required Subscriber information in terms of Section 3.2
- Payment (if applicable) has been received

An RA will reject a certificate application if:

- identification and authentication of all required Subscriber information in terms of Section 3.2 cannot be completed, or
- The Subscriber fails to furnish supporting documentation upon request
- The Subscriber fails to respond to notices within a specified time, or
- Payment (if applicable) has not been received, or
- The RA believes that issuing a certificate to the Subscriber MAY bring CERTISIGN TRUST NETWORK into disrepute

4.2.2.1. CABF Requirements for SSL Certificates

CERTISIGN TRUST NETWORK will not issue SSL Certificates containing a new gTLD under consideration by ICANN. Prior to issuing a Certificate containing an Internal Name with a gTLD that ICANN has announced as under consideration to make operational, CERTISIGN TRUST NETWORK MUST provide a warning to the applicant that the gTLD MAY soon become resolvable and that, at that time, CERTISIGN TRUST NETWORK will revoke the Certificate unless the applicant promptly registers the Domain Name. When a gTLD is delegated by inclusion in the IANA Root Zone Database, the Internal Name becomes a Domain Name, and at such time, a Certificate with such gTLD, which MAY have complied with these Requirements at the time it was issued, will be in a violation of these Requirements, unless CERTISIGN TRUST NETWORK has verified the Subscriber's rights in the Domain Name. The provisions below are intended to prevent such violation from happening.

Within 30 days after ICANN has approved a new gTLD for operation, as evidenced by publication of a contract with the gTLD operator on [www.ICANN.org] each CA will
(1) compare the new gTLD against the CA's records of valid certificates and
(2) cease issuing Certificates containing a Domain Name that includes the new gTLD until after CERTISIGN TRUST NETWORK has first verified the Subscriber's control over or exclusive right to use the Domain Name in accordance with Section 3.2.2.4.

Within 120 days after the publication of a contract for a new gTLD is published on [www.icann.org], CERTISIGN TRUST NETWORK will revoke each Certificate containing a Domain Name that includes the new gTLD unless the Subscriber is either the Domain Name Registrant or can demonstrate control over the Domain Name.

4.2.3 Time to Process Certificate Applications

CAs and RAs begin processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement between CERTISIGN TRUST NETWORK participants.

A certificate application remains active until rejected.

4.2.4 CABF Certificate Authority Authorization (CAA) Requirement

CERTISIGN checks Certificate Authority Authorization (CAA) records as part of its public SSL certificate authentication and verification processes. 'Public SSL Certificates' are those that are chain up to our publicly available root certificates and which meet CA/Browser Forum Baseline and Extended Validation Requirements.

4.3 Certificate Issuance

4.3.1 CA Actions during Certificate Issuance

A Certificate is created and issued following the approval of a Certificate Application by a CA or following receipt of an RA's request to issue the Certificate. CERTISIGN TRUST NETWORK creates and issues a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

Certificate issuance by the Root CA SHALL require an individual authorized by CERTISIGN TRUST NETWORK (i.e. CERTISIGN TRUST NETWORK system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notifications to Subscriber by a CA of Issuance of Certificate

CAs issuing Certificates to end-user Subscribers SHALL, either directly or through an RA, notify Subscribers that they have created such Certificates, and provide Subscribers with access to the Certificates by notifying them that their Certificates are available and the means for obtaining them. Certificates SHALL be made available to end-user Subscribers, either by allowing them to download them from a web site or via a message sent to the Subscriber containing the Certificate.

4.3.3 CABF Requirement for Certificate Issuance by a Root CA

Not applicable.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

The following conduct constitutes certificate acceptance:

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate.
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

CERTISIGN TRUST NETWORK publishs the Certificates it issues in a publicly accessible repository.

4.4.3 Notification of Certificate Issuance by a CA to Other Entities

RAs MAY receive notification of the issuance of certificates they approve.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Use of the Private Key corresponding to the public key in the certificate SHALL only be permitted once the Subscriber has agreed to the Subscriber Agreement and accepted the certificate. The certificate SHALL be used lawfully in accordance with CERTISIGN's Subscriber Agreement the terms of this CP and the relevant CPS. Certificate use MUST be consistent with the KeyUsage field extensions included in the certificate.

Subscribers SHALL protect their private keys from unauthorized use and SHALL discontinue use of the private key following expiration or revocation of the certificate. Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key except as set forth in section 4.12.

4.5.2 Relying Party Public Key and Certificate Usage

Relying parties SHALL assent to the terms of the applicable Relying Party Agreement as a condition of relying on the certificate.

Reliance on a certificate MUST be reasonable under the circumstances. If the circumstances indicate a need for additional assurances, the Relying Party MUST obtain such assurances for such reliance to be deemed reasonable.

Before any act of reliance, Relying Parties SHALL independently assess:

- the appropriateness of the use of a Certificate for any given purpose and determine that the Certificate will, in fact, be used for an appropriate purpose that is not prohibited or otherwise restricted by this CP. CERTISIGN, CAs, and RAs are not responsible for assessing the appropriateness of the use of a Certificate.
- that the certificate is being used in accordance with the KeyUsage field extensions included in the certificate.
- the status of the certificate and all the CAs in the chain that issued the certificate. If any of the Certificates in the Certificate Chain have been revoked, the Relying Party is solely responsible to investigate whether reliance on a digital signature performed by an end-user Subscriber Certificate prior to revocation of a Certificate in the Certificate chain is reasonable. Any such reliance is made solely at the risk of the Relying party.

Assuming that the use of the Certificate is appropriate, Relying Parties SHALL utilize the appropriate software and/or hardware to perform digital signature verification or other cryptographic operations they wish to perform, as a condition of relying on Certificates in connection with each such operation. Such operations include identifying a Certificate Chain and verifying the digital signatures on all Certificates in the Certificate Chain.

4.6 Certificate Renewal

Certificate renewal is the issuance of a new certificate to the subscriber without changing the public key or any other information in the certificate.

CERTISIGN TRUST NETWORK doesn´t allow certificate renewal.

4.6.1 Circumstances for Certificate Renewal

Not applicable.

4.6.2 Who May Request Renewal

Not applicable.

4.6.3 Processing Certificate Renewal Requests

Not applicable.

4.6.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Not applicable.

4.6.6 Publication of the Renewal Certificate by the CA

Not applicable.

4.6.7 Notification of Certificate Issuance a CA to Other Entities

Not applicable.

4.7 Certificate Re-Key

Certificate rekey is the application for the issuance of a new certificate that certifies the new public key.

4.7.1 Circumstances for Certificate Re-Key
Prior to the expiration of an existing Subscriber's Certificate, it is necessary for the Subscriber to re-key the certificate to maintain continuity of Certificate usage. A certificate may also be re-keyed after expiration.

4.7.2 Who May Request Certification of a New Public Key
Not applicable.

4.7.3 Processing Certificate Re-Keying Requests
Not applicable.

4.7.4 Notification of New Certificate Issuance to Subscriber
Not applicable.

4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate
Not applicable.

4.7.6 Publication of the Re-Keyed Certificate by the CA
Not applicable.

4.7.7 Notification of Certificate Issuance by a CA to Other Entities
Not applicable.

4.8 Certificate Modification

4.8.1 Circumstances for Certificate Modification
Certificate modification refers to the application for the issuance of a new certificate due to changes in the information in an existing certificate (other than the subscriber's public key).

Certificate modification is considered a Certificate Application in terms of Section 4.1.

4.8.2 Who May Request Certificate Modification
See Section 4.1.1

4.8.3 Processing Certificate Modification Requests
An RA SHALL perform identification and authentication of all required Subscriber information in terms of Section 3.2

4.8.4 Notification of New Certificate Issuance to Subscriber
See Section 4.3.2

4.8.5 Conduct Constituting Acceptance of Modified Certificate
See Section 4.4.1

4.8.6 Publication of the Modified Certificate by the CA
See Section 4.4.2

4.8.7 Notification of Certificate Issuance by a CA to Other Entities
See Section 4.4.3

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

CERTISIGN TRUST NETWORK SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that CERTISIGN TRUST NETWORK revoke the Certificate;
2. The Subscriber notifies CERTISIGN TRUST NETWORK that the original certificate request was not authorized and does not retroactively grant authorization;
3. CERTISIGN TRUST NETWORK obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
4. CERTISIGN TRUST NETWORK 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.

CERTISIGN TRUST NETWORK SHOULD revoke a certificate within 24 hours and MUST revoke a Certificate within 5 days if one or more of the following occurs:

1. The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
2. CERTISIGN TRUST NETWORK obtains evidence that the Certificate was misused;
3. CERTISIGN TRUST NETWORK is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
4. CERTISIGN TRUST NETWORK is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
5. CERTISIGN TRUST NETWORK is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
6. CERTISIGN TRUST NETWORK is made aware of a material change in the information contained in the Certificate;
7. CERTISIGN TRUST NETWORK is made aware that the Certificate was not issued in accordance with these Requirements or CERTISIGN TRUST NETWORK's Certificate Policy or Certification Practice Statement;
8. CERTISIGN TRUST NETWORK determines or is made aware that any of the information appearing in the Certificate is inaccurate;
9. CERTISIGN TRUST NETWORK's right to issue Certificates under these Requirements expires or is revoked or terminated, unless CERTISIGN TRUST NETWORK has made arrangements to continue maintaining the CRL/OCSP Repository;
10. Revocation is required by CERTISIGN TRUST NETWORK's Certificate Policy and/or Certification Practice Statement; or
11. CERTISIGN TRUST NETWORK is made aware of a demonstrated or proven method that exposes the Subscriber's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.

4.9.1.1.1 CABF Requirements

CERTISIGN TRUST NETWORK SHALL revoke a Certificate within 24 hours.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

1. The Subordinate CA requests revocation in writing;

2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
6. The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
7. The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
8. The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
9. Revocation is required by the Issuing CA's Certificate Policy and/or Certification Practice Statement.

4.9.2 Who Can Request Revocation

The Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties MAY submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.
Individual Subscribers can request the revocation of their own individual Certificates through an authorized representative of CERTISIGN or an RA.

In the case of organizational Certificates, a duly authorized representative of the organization SHALL be entitled to request the revocation of Certificates issued to the organization.

A duly authorized representative of CERTISIGN, an Affiliate, or a RA SHALL be entitled to request the revocation of an RA Administrator's Certificate.

The entity that approved a Subscriber's Certificate Application SHALL also be entitled to revoke or request the revocation of the Subscriber's Certificate.

Only CERTISIGN is entitled to request or initiate the revocation of the Certificates issued to its own CAs.

4.9.3 Procedure for Revocation Request

CERTISIGN TRUST NETWORK SHALL provide a process for Subscribers to request revocation of their own Certificates. The process MUST be described in CERTISIGN TRUST NETWORK's Certificate Policy or Certification Practice Statement. CERTISIGN TRUST NETWORK SHALL maintain a continuous 24x7 ability to accept and respond to revocation requests and Certificate Problem Reports.

CERTISIGN TRUST NETWORK SHALL provide Subscribers, Relying Parties, Application Software Suppliers, and other third parties with clear instructions for reporting suspected Private Key Compromise, Certificate misuse, or other types of fraud, compromise, misuse, inappropriate conduct, or any other matter related to Certificates. CERTISIGN TRUST NETWORK SHALL publicly disclose the instructions through a readily accessible online means and in section 1.5.2 of their CPS.

4.9.3.1 Procedure for Requesting the Revocation of an End-User Subscriber Certificate

Prior to the revocation of a Certificate, CERTISIGN TRUST NETWORK verifies that the revocation has been requested by the Certificate's Subscriber, or the entity that approved the Certificate Application. Acceptable procedures for authenticating Subscriber revocation requests include:

- Having the Subscriber for certain certificate types submit the Subscriber's Challenge Phrase (or an equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase (or an equivalent thereof) on record,
- Receiving a message purporting to be from the Subscriber that requests revocation and contains a digital signature verifiable with reference to the Certificate to be revoked, and
- Communication with the Subscriber providing reasonable that the person or organization requesting revocation is, in fact the Subscriber. Depending on the circumstances, such communication MAY include one or more of the following: telephone, facsimile, e-mail, postal mail, or courier service.

The requests from CAs to revoke a CA Certificate shall be authenticated by their Superior Entities to ensure that the revocation has in fact been requested by CERTISIGN TRUST NETWORK.

4.9.4 Revocation Request Grace Period

Revocation requests SHALL be submitted as promptly as possible within a commercially reasonable time.

4.9.5 Time within Which CA Must Process the Revocation Request

Within 24 hours after receiving a Certificate Problem Report, CERTISIGN TRUST NETWORK SHALL investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, CERTISIGN TRUST NETWORK SHALL work with the Subscriber and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which CERTISIGN TRUST NETWORK will revoke the certificate. The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation MUST NOT exceed the time frame set forth in Section 4.9.1.1. The date selected by CERTISIGN TRUST NETWORK SHOULD consider the following criteria:

1. The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
2. The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
3. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
4. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
5. Relevant legislation.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying Parties SHALL check the status of Certificates on which they wish to rely. One method by which Relying Parties MAY check Certificate status is by consulting the most recent CRL from CERTISIGN TRUST NETWORK that issued the Certificate on which the Relying Party wishes to rely. Alternatively, Relying Parties MAY meet this requirement either by checking Certificate status using the applicable web-based repository or by using OCSP (if available). CAs SHALL provide Relying Parties with information on how to find the appropriate CRL, web-based repository, or OCSP responder (where available) to check for revocation status.

A "CRL reference Table" is posted in the CERTISIGN Repository to enable Relying Parties to determine the location of the CRL for the relevant CA.

4.9.7 CRL Issuance Frequency

CRLs for end-user Subscriber Certificates are issued at least once per day. CRLs for CA Certificates SHALL be issued at least annually, but also within 24 hours whenever a CA Certificate is revoked.
Any deviation from this general policy MUST get approval from the PMD and be published in the appropriate CPS.

Subscriber Certificate Status Requirements

CERTISIGN TRUST NETWORK SHALL update and reissue CRLs at least once every 7 days, and the value of the *nextUpdate*field MUST NOT be more than 10 days beyond the value of the *thisUpdate*field.

Subordinate CA Certificate Status Requirements
CERTISIGN TRUST NETWORK SHALL update and reissue CRLs at least
(i) once every 12 months and
(ii) within 24 hours after revoking a Subordinate CA Certificate,
and the value of the *nextUpdate*field MUST NOT be more than 12 months beyond the value of the *thisUpdate*field.

4.9.8 Maximum Latency for CRLs

CRLs are posted to the CERTISIGN Repository within a commercially reasonable time after generation. This is generally done automatically within seconds of generation.

4.9.8.1 CABF Requirements for EV CRLs

CAs MUST ensure that CRLs for an EV Certificate chain can be downloaded in no more than 3 seconds over an analog telephone line under normal network conditions.

4.9.9 On-Line Revocation/Status Checking Availability

Online revocation and other Certificate status information are available via a web-based repository and, where offered, OCSP. Processing Centers shall have a web-based repository that permits Relying Parties to make online inquiries regarding revocation and other Certificate status information. A Processing Center, as part of its contract with a Service Center, shall host such a repository on behalf of the Service Center. Processing Centers provide Relying Parties with information on how to find the appropriate repository to check Certificate status and, if OCSP is available, how to find the correct OCSP responder.

OCSP responses MUST conform to RFC6960 and/or RFC5019. OCSP responses MUST either:
1. Be signed by CERTISIGN TRUST NETWORK, or
2. Be signed by an OCSP Responder whose Certificate is signed by CERTISIGN TRUST NETWORK. The OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

4.9.10 On-Line Revocation Checking Requirements

A relying party MUST check the status of a certificate on which he/she/it wishes to rely. If a Relying Party does not check the status of a Certificate on which the Relying Party wishes to rely by consulting the most recent relevant CRL, the Relying Party SHALL check Certificate status by consulting the applicable repository or by requesting Certificate status using the applicable OCSP responder (where OCSP services are available).

CERTISIGN TRUST NETWORK supports an OCSP capability using the GET method for Certificates issued in accordance with these Requirements.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder will not respond with a "good" status.

CERTISIGN TRUST NETWORK monitors the responder for such requests as part of its security response procedures.

4.9.10.1 CABF Requirements for OCSP

Certificate Status for Subscriber Certificates
CERTISIGN TRUST NETWORK SHALL update information provided via an Online Certificate Status Protocol at least every 4 days. OCSP responses from this service MUST have a maximum expiration time of 10 days

Certificate Status for Subordinate CA Certificates
CERTISIGN TRUST NETWORK SHALL update information provided via an Online Certificate Status Protocol at least (i) every 12 months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

4.9.11 Other Forms of Revocation Advertisements Available

If the Subscriber Certificate is for a high-traffic FQDN, CERTISIGN TRUST NETWORK relies on stapling, in accordance with RFC4366, to distribute its OCSP responses. In this case, CERTISIGN TRUST NETWORK ensures that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. CERTISIGN TRUST NETWORK enforces this requirement on the Subscriber either contractually, through the Subscriber Agreement or Terms of Use, or by technical review measures implemented by CERTISIGN TRUST NETWORK.

4.9.12 Special Requirements Regarding Key Compromise

CERTISIGN TRUST NETWORK Participants SHALL be notified of an actual or suspected CA private key Compromise using commercially reasonable efforts. CERTISIGN TRUST NETWORKs hall use commercially reasonable efforts to notify potential Relying Parties if they discover, or have reason to believe, that there has been a Compromise of the private key of one of their own CAs or one of the CAs within their sub-domain.

4.9.13 Circumstances for Suspension

Not applicable.

4.9.14 Who Can Request Suspension

Not applicable.

4.9.15 Procedure for Suspension Request

Not applicable.

4.9.16 Limits on Suspension Period

Not applicable.

4.9.16.1 CABF EV Code Signing Certificate Revocation and Status Checking Requirements

Additionally as specified in Section 4.9:

(A) Revocation Reasons: Subscribers are expected to not intentionally include Suspect Code in their signed software. Intentionally signing Suspect Code is a violation of the terms of the Subscriber Agreement, and will likely result in revocation of the EV Code Signing Object.

(B) Revocation Status Information: Certification Authorities are required to provide accurate and up-to-date revocation status information for at least one year following the expiration of the associated certificate. The CA SHALL, upon request, provide accurate and up-to-date revocation status information for a period not less than one year beyond expiry of the EV Code Signing Certificate.

(C) Revocation Processing: Whenever practical, platforms should check the revocation status of the certificates that they rely upon. However, this is not always practical. This situation occurs, for instance, when signed code has to be loaded earlier in the boot sequence than the network communication stack.

In the timestamp model, the platform should deviate from the RFC 5280 certification path validation algorithm and check the revocation status, not only of the timestamp certificate, but also of the Subscriber's EV Code Signing Certificate at the time of reliance rather than at the time the time-stamp was applied.

In addition to checking revocation status, where practical, platforms should consult blacklists of suspect software.

(D) Revocation Consequences: A certificate may have a one-to-one relationship with the software object that it verifies. In such cases, revocation of the certificate only invalidates the signature on the code that is suspect. If, on the other hand, a certificate has a one-to-many relationship with the software objects that it verifies, then revocation of the certificate invalidates the signatures on all those software objects, some of which may be perfectly sound.

(E) Responsiveness. CERTISIGN TRUST NETWORK SHALL respond to all plausible notices that a signed software object containing Suspect Code verifies with a certificate that it has issued by setting the revocation status of that certificate to 'revoked'.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of public certificates is available via CRL through CERTISIGN TRUST NETWORK website (at a URL specified in AC's CPS) and via an OCSP responder (where available).

Revocation entries on a CRL or OCSP Response MUST NOT be removed until "Expiry Date" of the revoked Certificate.

4.10.2 Service Availability

CERTISIGN TRUST NETWORK operates and maintains its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

CERTISIGN TRUST NETWORK maintains an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by it.

CERTISIGN TRUST NETWORK maintains 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.

4.10.3 Optional Features

OCSP is an OPTIONAL status service feature that is not available for all products and MUST be specifically enabled for other products.

4.11 End of Subscription

A subscriber MAY end a subscription for a CERTISIGN TRUST NETWORK certificate by:

- Allowing his/her/its certificate to expire without renewing or re-keying that certificate
- Revoking of his/her/its certificate before certificate expiration without replacing the certificate.

4.12 Key Escrow and Recovery

No CERTISIGN TRUST NETWORK participant MAY escrow CA, RA or end-user Subscriber private keys.

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

CERTISIGN TRUST NETWORK develops, implements and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability of Certificate Data and Certificate Management Processes;
2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;
3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;
4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and
5. Comply with all other security requirements applicable to CERTISIGN TRUST NETWORK by law.

The Certificate Management Process includes:
1. physical security and environmental controls;
2. system integrity controls, including configuration management, integrity maintenance of trusted code, and malware detection/prevention;
3. network security and firewall management, including port restrictions and IP address filtering;
4. user management, separate trusted-role assignments, education, awareness, and training; and
5. logical access controls, activity logging, and inactivity time-outs to provide individual accountability.

CERTISIGN TRUST NETWORK security program includes an annual Risk Assessment that:
1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that CERTISIGN TRUST NETWORK has in place to counter such threats.

Based on the Risk Assessment, CERTISIGN TRUST NETWORK develops, implements and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUSTinclude administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical Controls

CERTISIGN has implemented the CERTISIGN Physical Security Policy, which supports the security requirements of this CPS. Compliance with these policies is included in CERTISIGN 's independent audit requirements described in Section 8.

CERTISIGN Physical Security Policy contains sensitive security information and is only available upon agreement with CERTISIGN. An overview of the requirements are described in the subsections following.

5.1.1 Site Location and Construction

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

CERTISIGN also maintains disaster recovery facilities for its CA operations. CERTISIGN 's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of CERTISIGN 's primary facility.

5.1.2 Physical Access

CERTISIGN TRUST NETWORK CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier REQUIRED before gaining access to the higher tier.

Progressively restrictive physical access privileges control access to each tier.

5.1.2.1. Sensitive CA operational activity

Any activity related to the lifecycle of the certification process occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including

biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas.

The physical security system includes additional tiers for key management security which serves to protect both online and offline storage ofCERTISIGN TRUST NETWORK CA cryptographic hardwares and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online & offline CA cryptographic hardwaresare protected through the use of locked safes, cabinets and containers.

Access to CA cryptographic hardwaresand keying material is restricted in accordance with CERTISIGN 's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes.

5.1.3 Power and Air Conditioning

CERTISIGN 's secure facilities are equipped with primary and backup:

- power systems to ensure continuous, uninterrupted access to electric power and
- heating/ventilation/air conditioning systems to control temperature and relative humidity.

5.1.4 Water Exposures

CERTISIGN safe facility minimize the impact of water exposure to CERTISIGN systems.

5.1.5 Fire Prevention and Protection

CERTISIGN has taken reasonable precautions to prevent and extinguish fires or other damaging exposure to flame or smoke. CERTISIGN 's fire prevention and protection measures have been designed to comply with local fire safety regulations.

5.1.6 Media Storage

All media containing production software and data, audit, archive, or backup information is stored within CERTISIGN 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 zeroized in accordance the manufacturers' guidance prior to disposal.

Other waste is disposed of in accordance with CERTISIGN 's normal waste disposal requirements.

5.1.8 Off-Site Backup

CERTISIGN performs routine backups of critical system data, audit log data, and other sensitive information. Offsite backup media are stored in a physically secure manner using a third party storage facility and CERTISIGN's disaster recovery facility.

5.2 Procedural Controls

5.2.1 Trusted Roles

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

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, renewal requests, or enrollment information;

- the issuance, or revocation of Certificates, including personnel having access to restricted portions of its repository;
- the handling of Subscriber information or requests.

Trusted Persons include, but are not limited to:

- cryptographic operations personnel,
- security personnel,
- system administration personnel,
- designated engineering personnel, and
- executives that are designated to manage infrastructural trustworthiness.

CERTISIGN 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 MUST successfully complete the screening requirements set out in this CPS.

5.2.2 Number of Persons Required per Task

CERTISIGN 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 and associated key material, require multiple Trusted Persons.

These internal control procedures are designed to ensure that at a minimum, two trusted personnel 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. Persons with physical access to modules do not hold “Secret Shares” and vice versa.

Other manual operations require the participation of at least two (2) Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process. Manual operations for Key Recovery MAY optionally require the validation of two (2) authorized Administrators.

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 CERTISIGN HR or security functions and a check of well-recognized forms of identification. Identity is further confirmed through the background checking procedures in CPS Section 5.3.1.

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

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

5.2.4 Roles Requiring Separation of Duties

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

- the validation of information in Certificate Applications;
- the acceptance, rejection, or other processing of Certificate Applications, revocation requests, key recovery requests or renewal requests, or enrollment information;

- the issuance, or revocation of Certificates, including personnel having access to restricted portions of the repository;
- the handling of Subscriber information or requests;
- the generation, issuing or destruction of a CA certificate;
- the loading of a CA to a Production environment.

5.2.4.1. CABF Requirements for Separation of Duties for EV

(1) CERTISIGN MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in CP Appendix C, item 13, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.
(2) Such controls MUST be auditable.

5.3 Personnel Controls

This section applies to both CAs and Signing Authorities.

Personnel seeking to become Trusted Persons MUST present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily. Background checks are repeated at least every 5 years for personnel holding Trusted Positions.

5.3.1 Qualifications, Experience, and Clearance Requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of CERTISIGN. CERTISIGN SHALL verify the identity and trustworthiness of such person. CERTISIGN requires that personnel seeking to become Trusted Persons present proof of the requisite background, qualifications, and experience needed to perform their prospective job responsibilities competently and satisfactorily.

5.3.1.1. CABF Requirements for Identity and Background Verification for EV

Prior to the commencement of employment of any person by CERTISIGN for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of CERTISIGN, CERTISIGN MUST:
(1) Verify the Identity of Such Person: Verification of identity MUST be performed through:

(A) The personal (physical) presence of such person before trusted persons who perform human resource or security functions, and
(B) The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses); and

(2) Verify the Trustworthiness of Such Person: Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:

(A) Confirmation of previous employment,
(B) Check of professional references;
(C) Confirmation of the highest or most-relevant educational qualification obtained;
(D) Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed; and

(3) In the case of employees already in the employ of CERTISIGN at the time of adoption of this Section whose identity and background has not previously been verified as set forth above, CERTISIGN SHALL conduct such verification within three months of the date of adoption of it.

5.3.2 Background Check Procedures

Prior to commencement of employment in a Trusted Role, CERTISIGN conducts background checks which include the following:

- confirmation of previous employment,

- check of professional reference,
- confirmation of the highest or most relevant educational degree obtained,
- search of criminal records,
- check of credit/financial records,

Reports containing information about factors revealed in a background check are evaluated by human resources and security personnel, who determine the appropriate course of action in light of the type, magnitude, and frequency of the behavior uncovered by the background check. Such actions MAY include measures up to and including the cancellation of offers of employment made to candidates for Trusted Positions or the termination of existing Trusted Persons.

5.3.3 Training Requirements

CERTISIGN provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily.

CERTISIGN maintains records of such training. CERTISIGN periodically reviews and enhances its training programs as necessary.

CERTISIGN 's training programs are tailored to the individual's responsibilities and include the following as relevant:

- Basic PKI concepts,
- Job responsibilities,
- CERTISIGN security and operational policies and procedures,
- Use and operation of deployed hardware and software,
- Incident and Compromise reporting and handling, and
- Disaster recovery and business continuity procedures.

5.3.3.1 CABF Requirements for Training and Skill Level

Addition to the requirements in Section 5.3.3, CERTISIGN SHALL provide all personnel performing information verification duties with skills-training that covers:

- authentication and vetting policies and procedures (including CERTISIGN CP and/or CPS),
- common threats to the information verification process (including phishing and other social engineering tactics), and
- CABFORUM Requirements.

CERTISIGN SHALL maintain records of such training and ensure that personnel entrusted with Validation Specialist duties maintain a skill level that enables them to perform such duties satisfactorily.

CERTISIGN SHALL document that each Validation Specialist possesses the skills required by a task before allowing the Validation Specialist to perform that task.

CERTISIGN SHALL require all Validation Specialists to pass an examination provided by CERTISIGN on the information verification requirements outlined in CABFORUM Requirements.

5.3.3.1.1CABF Requirements for Training and Skill Level for EV

The requirements in Section 5.3.3 and 5.3.3.1. apply equally to EV Certificates. The required internal examination MUST relate to the EV Certificate validation criteria outlined in it.

5.3.4 Retraining Frequency and Requirements

CERTISIGN provides refresher training and updates to their personnel to the extent and frequency required to ensure that such personnel maintain the required level of proficiency to perform their job responsibilities competently and satisfactorily.

5.3.5 Job Rotation Frequency and Sequence
Not applicable.

5.3.6 Sanctions for Unauthorized Actions
Appropriate disciplinary actions are taken for unauthorized actions or other violations of CERTISIGN policies and procedures. Disciplinary actions MAY include measures up to and including termination and are commensurate with the frequency and severity of the unauthorized actions.

5.3.7 Independent Contractor Requirements
In limited circumstances, independent contractors or consultants MAY be used to fill Trusted Positions. Any such contractor or consultant is held to the same functional and security criteria that apply to a CERTISIGN employees in a comparable position.

CERTISIGN SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.3 and the document retention and event logging requirements of Section 5.4.1.

Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS Section 5.3.2 are permitted access to CERTISIGN 's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.

5.3.7.1. CABF Requirements for Delegation of Functions to Registration Authorities and Subcontractors for EV and EV Code Signing Certificates
CERTISIGN MAY delegate the performance of all or any part of a requirement to an Affiliate or a Registration Authority (RA) or subcontractor, provided that the process employed by the CA fulfills all of the requirements listed in CP Appendix C, Item 13. Affiliates and/or RAs MUST comply with the qualification requirements of Section 5.3.1.1.
CERTISIGN SHALL verify that the Delegated Third Party's personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 5.3.1.1.1. and the document retention and event logging requirements of Section 5.4.3.1.

5.3.7.1.1. Enterprise RAs

5.3.7.1.1.1. EV Requirements
CERTISIGN MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize CERTISIGN to issue additional EV Certificates at third and higher domain levels that are contained within the domain of the original EV Certificate (also known as an Enterprise EV Certificate). In such case, the Subject SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

(1) An Enterprise RA SHALL NOT authorize CERTISIGN to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;
(2) In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by CERTISIGN in accordance with this CPS;
(3) CERTISIGN MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;
(4) The Final Cross-Correlation and Due Diligence requirements of CP Appendix C, Item 13 of these Guidelines MAY be performed by a single person representing the Enterprise RA; and
(5) The audit requirements of this CPS SHALL apply to the Enterprise RA, except in the case where CERTISIGN maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA MAY be exempted from the audit requirements.

5.3.7.1.1.2. EV Code Signing Requirements

The CA MAY NOT contractually authorize the Subject of a specified Valid EV Code Signing Certificate to perform the RA function and authorize the CA to issue additional EV Code Signing Certificates.

5.3.7.1.2. Guidelines Compliance Obligation

In all cases, CERTISIGN MUST contractually obligate each Affiliate, RA, subcontractor, and Enterprise RA to comply with all applicable requirements in this CPS, its CP and to perform them as required of CERTISIGN itself. CERTISIGN SHALL enforce these obligations and internally audit each Affiliate's, RA's, subcontractor's, and Enterprise RA's compliance with these Requirements on an annual basis.

5.3.7.1.3. Allocation of Liability

As specified in Section 9.8.

5.3.8 Documentation Supplied to Personnel

CERTISIGN provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

5.4 Audit Logging Procedures

5.4.1 Types of Events Recorded

CERTISIGN and each Delegated Third Party SHALL record details of the actions taken to process a certificate request and to issue a Certificate, including all information generated and documentation received in connection with the certificate request; the time and date; and the personnel involved. CERTISIGN SHALL make these records available to its Qualified Auditor as proof of the CERTISIGN compliance with CABFORUM Requirements.

CERTISIGN manually or automatically logs the following significant events:

- CA key life cycle management events, including:
  - Key generation, backup, storage, recovery, archival, and destruction
  - Cryptographic device life cycle management events.
- CA and Subscriber certificate life cycle management events, including:
  - Certificate Applications, renewal, rekey, and revocation
  - Successful or unsuccessful processing of requests
  - Generation and issuance of Certificates and CRLs.
- Security-related events including:
  - Successful and unsuccessful PKI system access attempts
  - PKI and security system actions performed by CERTISIGN personnel
  - Security sensitive files or records read, written or deleted
  - Security profile changes
  - System crashes, hardware failures and other anomalies
  - Firewall and router activity
  - CA facility visitor entry/exit.

Log entries include the following elements:

- Date and time of the entry
- Serial or sequence number of entry, for automatic journal entries
- Identity of the entity making the journal entry
- Description/kind of entry.

CERTISIGN RAs and Enterprise Administrators log Certificate Application information including:

- Kind of identification document(s) presented by the Certificate Applicant

- Record of unique identification data, numbers, or a combination thereof of identification documents, if applicable
- Storage location of copies of applications and identification documents
- Identity of entity accepting the application
- Method used to validate identification documents, if any
- Name of receiving CA or submitting RA, if applicable.

5.4.1.1 CABF Types of Events Recorded Requirements

Additionally, CERTISIGN manually or automatically logs the following significant events:

- CA and Subscriber certificate life cycle management events, including:
    - All verification activities stipulated in CABFORUM Requirements and this CPS;
    - Date, time, phone number used, persons spoken to, and end results of verification telephone calls;
    - OCSP responses.

5.4.2 Frequency of Processing Log

CERTISIGN system is continuously monitored to provide real time alerts of significant security and operational events for review by designated system security personnel. Monthly reviews of the audit logs include verifying that the logs have not been tampered with and thoroughly investigating any alerts or irregularities detected in the logs. Actions taken based on audit log reviews are also documented.

5.4.3 Retention Period for Audit Log

Audit logs SHALL be retained onsite for at least 2 months after processing and thereafter archived in accordance with Section 5.5.2.

5.4.3.1 CABF Retention Period for Audit Log Requirements

CERTISIGN SHALL retain any audit logs generated for at least seven years. CERTISIGN SHALL make these audit logs available to its Qualified Auditor upon request.

5.4.4 Protection of Audit Log

Audit logs are protected with an electronic audit log system that includes mechanisms to protect the log files from unauthorized viewing, modification, deletion, or other tampering.

5.4.5 Audit Log Backup Procedures

Incremental backups of audit logs are created daily and full backups are performed monthly.

5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application, network and operating system level. Manually generated audit data is recorded by CERTISIGN personnel.

5.4.7 Notification to Event-Causing Subject

Where an event is logged by the audit collection system, no notice is REQUIRED to be given to the individual, organization, device, or application that caused the event.

5.4.8 Vulnerability Assessments

Events in the audit process are logged, in part, to monitor system vulnerabilities. Logical security vulnerability assessments ("LSVAs") are performed, reviewed, and revised following an examination of these monitored events. LSVAs are based on real-time automated logging data and are performed on a daily, weekly, monthly or annual basis. An annual LSVA will be an input into an entity's annual Compliance Audit.

Additionally, CERTISIGN security program MUST include an annual Risk Assessment that:
1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure,

misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that CERTISIGN has in place to counter such threats

5.5 Records Archival

5.5.1 Types of Records Archived

CERTISIGN archives:

- All audit data collected in terms of Section 5.4
- Certificate application information
- Documentation supporting certificate applications
- Certificate lifecycle information e.g., revocation, rekey and renewal application information

5.5.2 Retention Period for Archive

CERTISIGN SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for at least seven years after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of Archive

CERTISIGN protects the archive so that only authorized Trusted Persons are able to obtain access to the archive. The archive is protected against unauthorized viewing, modification, deletion, or other tampering by storage within a Trustworthy System. The media holding the archive data and the applications REQUIRED to process the archive data SHALL be maintained to ensure that the archive data can be accessed for the time period set forth in this CPS.

5.5.4 Archive Backup Procedures

CERTISIGN incrementally backs up electronic archives of its issued Certificate information on a daily basis and performs full backups on a montly basis. Copies of paper-based records SHALL be maintained in an off-site secure facility.

5.5.5 Requirements for Time-Stamping of Records

Certificates, CRLs, and other revocation database entries SHALL contain time and date information.

Such time information need not be cryptographic-based.

5.5.6 Archive Collection System (Internal or External)

CERTISIGN archive collection systems are internal, except for enterprise RA Customers. CERTISIGN assists its enterprise RAs in preserving an audit trail. Such an archive collection system therefore is external to that enterprise RA.

5.5.7 Procedures to Obtain and Verify Archive Information

Only authorized Trusted Personnel are able to obtain access to the archive. The integrity of the information is verified when it is restored.

5.6 Key Changeover

CERTISIGN TRUST NETWORK CA key pairs are retired from service at the end of their respective maximum lifetimes as defined in this CPS.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

Backups of the following CA information SHALL be kept in off-site storage and made available in the event of a Compromise or disaster:

- Certificate Application data,
- audit data, and
- database records for all Certificates issued.

Backups of CA private keys SHALL be generated and maintained in accordance with CP Section 6.2.4. CERTISIGN maintains backups of the foregoing CA information for their own CAs, as well as the CAs of Enterprise Customers within its Sub-domain.

CERTISIGN TRUST NETWORK has an Incident Response Plan and a Disaster Recovery Plan.
CERTISIGN TRUST NETWORK documents a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster,
security compromise, or business failure.
CERTISIGN TRUST NETWORK is not REQUIRED to publicly disclose its business continuity plans but makes its business continuity plan and security plans available to its auditors upon request. CERTISIGN TRUST NETWORK annually tests, reviews and updates these procedures.

The business continuity plan includes:
1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;
6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. CERTISIGN TRUST NETWORK plan to maintain or restore the its business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials at an alternate location;
12. What constitutes an acceptable system outage and recovery time;
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to CERTISIGN TRUST NETWORK main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

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

In the event of the corruption of computing resources, software, and/or data, such an occurrence is reported to CERTISIGN Security and CERTISIGN 's incident handling procedures are enacted. Such procedures require appropriate escalation, incident investigation, and incident response. If necessary, CERTISIGN 's key compromise or disaster recovery procedures will be enacted.

5.7.3 Entity Private Key Compromise Procedures

Upon the suspected or known Compromise of a CERTISIGN TRUST NETWORK CA, CERTISIGN infrastructure or Customer CA private key, CERTISIGN 's Key Compromise Response procedures are enacted by the CERTISIGN Security Incident Response Team. This team, which includes Security, Cryptographic Business Operations,

Production Services personnel, and other CERTISIGN management representatives, assesses the situation, develops an action plan, and implements the action plan with approval from CERTISIGN executive management.

If CA Certificate revocation is REQUIRED, the following procedures are performed:

- The Certificate's revoked status is communicated to Relying Parties through the CERTISIGN Repository in accordance with Section 4.9.7,
- Commercially reasonable efforts will be made to provide additional notice of the revocation to all affected CERTISIGN TRUST NETWORK Participants, and
- The CA will generate a new key pair in accordance with Section 5.6, except where the CA is being terminated in accordance with Section 5.8.

5.7.4 Business Continuity Capabilities after a Disaster

CERTISIGN has created and maintains business continuity plans so that in the event of a business disruption, critical business functions MAY be resumed. CERTISIGN maintains a Disaster Recovery Facility (DRF) located at a facility geographically separate from the primary Production Facility.

The DRF is equipped to meet this CPS security standards.

In the event of a natural or man-made disaster requiring permanent cessation of operations fromCERTISIGN 's primary facility, the Corporate CERTISIGN Business Continuity Team and the CERTISIGN Authentication Operations Incident Management Team will coordinate with cross functional management teams to make the decision to formally declare a disaster situation and manage the incident. Once a disaster situation is declared, restoration of CERTISIGN 's Production services functionality at the DRF will be initiated.

CERTISIGN has developed a Disaster Recovery Plan (DRP) for its managed PKI services including CERTISIGN TRUST NETWORK PKI service. The DRP identifies conditions for activating the plan and what constitutes an acceptable system outage and recovery time. The DRP defines the procedures for the teams to reconstitute CERTISIGN CERTISIGN TRUST NETWORK operations using backup data and backup copies of CERTISIGN TRUST NETWORK keys.

CERTISIGN TRUST NETWORK entities operating secure facilities for CA and RA operations develop, test, maintain and, if necessary, implement a Disaster Recovery Plan (DRP) designed to mitigate the effects of any kind of natural or man-made disaster. The DRP SHALL identify conditions for activating the plan and what constitutes an acceptable system outage and recovery time for the restoration of information systems services and key business functions within a defined recovery time objective (RTO).

Additionally, the DRP SHALL include:

- Frequency for taking backup copies of essential business information and software,
- Requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location,
- Separation distance of the Disaster recovery site to the CA's main site,
- Procedures for securing the Disaster facility during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

The DRP SHALL include administrative requirements including:

- maintenance schedule for the plan;
- Awareness and education requirements;
- Responsibilities of the individuals; and
- Regular testing of contingency plans.

Disaster recovery sites have the equivalent physical security protections specified by CERTISIGN TRUST NETWORK.

CERTISIGN TRUST NETWORK has the capability of restoring or recovering essential operations within 48 hours following a disaster with, at a minimum, support for the following functions:

- certificate issuance,
- certificate revocation,
- publication of revocation information, and
- providing key recovery information for Enterprise Customers using Certigate.

CERTISIGN TRUST NETWORK's disaster recovery database SHALL be synchronized with the production database within the time limits set forth in the Security and Audit Requirements Guide. CERTISIGN TRUST NETWORK's disaster recovery equipment SHALL have the physical security protections documented in CERTISIGN TRUST NETWORK's confidential security policies, which includes the enforcement of physical security tiers.

5.7.4.1 CABF Requirements for Business Continuity Capabilities after a Disaster

Not applicable.

5.7.4.1.1 CABF Requirements for Business Continuity Capabilities after a Disaster for EV

Not applicable.

5.8 CA or RA Termination

In the event that it is necessary for a CERTISIGN TRUST NETWORK CA, or Enterprise Customer CA to cease operation, CERTISIGN makes a commercially reasonable effort to notify Subscribers, Relying Parties, and other affected entities of such termination in advance of the CA termination. Where CA termination is REQUIRED, CERTISIGN and, in the case of a Customer CA, the applicable Customer, will develop a termination plan to minimize disruption to Customers, Subscribers, and Relying Parties. Such termination plans MAY address the following, as applicable:

- Provision of notice to parties affected by the termination, such as Subscribers, Relying Parties, and Customers, informing them of the status of the CA,
- Handling the cost of such notice,
- The revocation of the Certificate issued to the CA by CERTISIGN,
- The preservation of the CA's archives and records for the time periods REQUIRED in this CPS,
- The continuation of Subscriber and customer support services,
- The continuation of revocation services, such as the issuance of CRLs or the maintenance of online status checking services,
- The revocation of unexpired unrevoked Certificates of end-user Subscribers and subordinate CAs, if necessary,
- Refunding (if necessary) Subscribers whose unexpired unrevoked Certificates are revoked under the termination plan or provision, or alternatively, the issuance of replacement Certificates by a successor CA,
- Disposition of the CA's private key and the hardware tokens containing such private key, and
- Provisions needed for the transition of the CA's services to a successor CA.

5.9 Data Security

Both CAs and Signing Authorities are required to abide by the obligations under this Section.

5.9.1 Objectives

CERTISIGN develops, implements, and maintains a comprehensive security program designed to:

1. Protect the confidentiality, integrity, and availability (CIA) of Certificate Data and Certificate Management Processes;

2. Protect against anticipated threats or hazards to the confidentiality, integrity, and availability of the Certificate Data and Certificate Management Processes;

3. Protect against unauthorized or unlawful access, use, disclosure, alteration, or destruction of any Certificate Data or Certificate Management Processes;

4. Protect against accidental loss or destruction of, or damage to, any Certificate Data or Certificate Management Processes; and

5. Comply with all other security requirements applicable to the CA by law.

5.9.2 Risk Assessment

CERTISIGN performs an annual Risk Assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any Certificate Data or Certificate Management Processes;

2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and

3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the CA has in place to counter such threats.

5.9.3 Security Plan

Based on results of the annual Risk Assessment, CERTISIGN develops, implements, and maintains a Security Plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes.

The Security Plan includes administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The Security Plan takes into account then-available technology and the cost of implementing the specific measures, and implements a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.9.4. Data Security for EV

The requirements of this Section apply to CAs and Signing Authorities.

Additionally, systems used to process and approve EV Code Signing Certificate and EV Signature requests MUST require actions by at least two trusted persons before creating an EV Code Signing Certificate or EV Signature.

In addition:
(1) An EV Timestamp Authority MUST protect its Private Key in a crypto module validated in accordance with FIPS 140-2 Level 2.

(2) An EV Timestamp Authority MUST be synchronized with a UTC(k) time source recognized by the International Bureau of Weights and Measures (BIPM).

(3) Signing Authorities shall protect private keys in a FIPS 140-2 level 2 (or equivalent) crypto module. Techniques that may be used to satisfy this requirement include:
a. Use of an HSM, verified by means of a manufacturer's certificate;

b. A hardware crypto module provided by the CA;

c. Contractual terms in the subscriber agreement requiring the Subscriber to protect the private key to a standard equivalent to FIPS 140-2 and with compliance being confirmed by means of an audit.

d. Cryptographic algorithms, key sizes and certificate life-times for both authorities and Subscribers are governed by the NIST key management guidelines.

(4) CAs SHALL ensure that the Subscriber's private key is generated, stored and used in a crypto module that meets or exceeds the requirements of FIPS 140-2 level 2. Acceptable methods of satisfying this requirement include (but are not limited to) the following:

a. The CA ships a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar;

b. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the key is managed in a suitable hardware module;

c. The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Key pair generation SHALL be performed using Trustworthy Systems and processes that provide the required cryptographic strength of the generated keys and prevent the loss, disclosure, modification, or unauthorized use of private keys. This requirement applies to end-user Subscribers, Enterprise Customers using Certigate, CAs pre-generating key pairs on end-user Subscriber hardware tokens.

CA key pair generation is performed by multiple pre-selected, trained and trusted individuals using Trustworthy Systems and processes that provide for the security and REQUIRED cryptographic strength for the generated keys.

For CERTISIGN ROOT CERTIFICATION AUTHORITY and Issuing Root CAs, the cryptographic modules used for key generation meet the requirements of FIPS 140-1 level 3 or other similar standard used in Brazil.

All CA key pairs are generated in pre-planned Key Generation Ceremonies in accordance with CERTISIGN internal requirements. The activities performed in each key generation ceremony are recorded, dated and signed by all individuals involved. These records are kept for audit and tracking purposes for a length of time deemed appropriate by CERTISIGN Management.

CERTISIGN TRUST NETWORK maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and its Key Generation Script.

CERTISIGN recommends that Automated Administration server key pair generation be performed using a FIPS 140-1 level 2 certified cryptographic module or other similar standard used in Brazil.

Generation of end-user Subscriber key pairs is generally performed by the Subscriber. The Subscriber typically uses a FIPS 140-1 level 1 certified cryptographic module provided with their browser software for key generation. For server Certificates, the Subscriber typically uses the key generation utility provided with the web server software.

6.1.1.1. CABF CA Key Pair Generation Requirements

For Root CA Key Pairs created that are either (i) used as Root CA Key Pairs or (ii) Key Pairs generated for a subordinate CA that is not the operator of the Root CA or an Affiliate of the Root CA, CERTISIGN TRUST NETWORK SHALL:

1. prepare and follow a Key Generation Script,
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process, and
3. have a Qualified Auditor issue a report opining that the CA followed its key ceremony during its Key and Certificate generation process and the controls used to ensure the integrity and confidentiality of the Key Pair.

For other CA Key Pairs that are for the operator of the Root CA or an Affiliate of the Root CA, CERTISIGN TRUST NETWORK SHOULD:

1. prepare and follow a Key Generation Script and
2. have a Qualified Auditor witness the Root CA Key Pair generation process or record a video of the entire Root CA Key Pair generation process.

In all cases, CA CERTISIGN TRUST NETWORK:

1. generates the keys in a physically secured environment as described in this CP and/or CPS;
2. generates CERTISIGN TRUST NETWORK keys using personnel in trusted roles under the principles of multiple person control and split knowledge;

3. generates CERTISIGN TRUST NETWORK keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in in this CP and/or CPS;
4. logs its CA key generation activities; and
5. maintains effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in this CP and/or CPS.

6.1.2 Private Key Delivery to Subscriber

End-user Subscribers' private keys are generally generated by the end-user Subscribers themselves, and therefore private key delivery to a Subscriber is unnecessary. Private keys SHALL be delivered to end-user Subscribers only when:

- Their Certificate Applications are approved by an Enterprise Customer using Certigate, or
- Their key pairs are pre-generated on hardware tokens, which are distributed to Certificate Applicants in connection with the enrollment process. Enterprise Customers MUST use Trustworthy Systems to deliver private keys to Subscribers and MUST secure such delivery through the use of a PKCS#12 package or any other comparably equivalent means (e.g., encryption) in order to prevent the loss, disclosure, modification, or unauthorized use of such private keys. Where key pairs are pre-generated on hardware tokens, the entities distributing such tokens MUST take commercially reasonable efforts to provide physical security of the tokens to prevent the loss, disclosure, modification, or unauthorized use of the private keys on them.

Parties other than the Subscriber SHALL NOT archive the Subscriber Private Key without authorization by the Subscriber.

If CERTISIGN TRUST NETWORK or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then CERTISIGN TRUST NETWORK SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If CERTISIGN TRUST NETWORK or any of its designated RAs generated the Private Key on behalf of the Subscriber, then CERTISIGN TRUST NETWORK SHALL encrypt the Private Key for transport to the Subscriber.

6.1.3 Public Key Delivery to Certificate Issuer

When a public key is transferred to the issuing CA to be certified, it SHALL be delivered through a mechanism ensuring that the public key has not been altered during transit and that the Certificate Applicant possesses the private key corresponding to the transferred public key. The acceptable mechanism within CERTISIGN TRUST NETWORK for public key delivery is a PKCS#10 Certificate signing request package or an equivalent method ensuring that:

- The public key has not been altered during transit; and
- The Certificate Applicant possesses the private key corresponding to the transferred public key.

CERTISIGN TRUST NETWORK performing Key Generation Ceremonies transfer the public key from the cryptographic module where it was created to the cryptographic module of the superior CA (same cryptographic module if a CCA) by wrapping it in a PKCS#10 Certificate signing request.

6.1.4 CA Public Key Delivery to Relying Parties

CERTISIGN provides the full certificate chain (including the issuing CA and any CAs in the chain) to the end-user Subscriber upon Certificate issuance. CERTISIGN TRUST NETWORK CA Certificates MAY also be downloaded from http://ctn.certisign.com.br/ctn/certisign-trust-network.htm.

CERTISIGN make reasonable effort to the public keys of the CERTISIGN TRUST NETWORK be included in Root Certificates that are already embedded within many popular software applications, making special root distribution mechanisms unnecessary. Also, in many instances, a Relying Party using the S/MIME protocol will automatically receive, in addition to the Subscriber's Certificate, the Certificates (and therefore the public keys) of all CAs subordinate to CERTISIGN TRUST NETWORK .

6.1.5 Key Sizes

Key pairs SHALL be of sufficient length to prevent others from determining the key pair's private key using cryptanalysis during the period of expected utilization of such key pairs.

CERTISIGN TRUST NETWORK Standard is:

- key sizes for end-users: 2048 bit RSA
- digital signature hash algorithm: SHA-2

6.1.5.1 CABF Requirements for Key Sizes

This information aplies to Root CA Certificates , Subordinate CA Certificates and Subscriber Certificates

Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits) *	L= 2048, N= 224 or L= 2048, N= 256

* L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-4 (http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf).

6.1.5.1.1 CABF Requirements for Key Sizes for EV

Not applicable.

6.1.6 Public Key Parameters Generation and Quality Checking

CERTISIGN TRUST NETWORK Participants SHALL generate the required Key Parameters in accordance a PMD-approved equivalent standard.
The same standards SHALL be used to check the quality of the generated Key Parameters.

RSA: CERTISIGN TRUST NETWORK SHALL confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent SHOULD be in the range between $2^{16}+1$ and $2^{256}-1$. The modulus SHOULD also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].

DSA: Although FIPS 800-57 says that domain parameters MAY be made available at some accessible site, compliant DSA certificates MUST include all domain parameters. This is to insure maximum interoperability among relying party software. CERTISIGN TRUST NETWORK MUST confirm that the value of the public key has the unique correct representation and range in the field, and that the key has the correct order in the subgroup. [Source: Section 5.3.1, NIST SP 800-89].

ECC: CERTISIGN TRUST NETWORK SHOULD confirm the validity of all keys using either the ECC Full Public Key Validation Routine or the ECC Partial Public Key Validation Routine. [Source: Sections 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 56A: Revision 2].

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

Private Keys corresponding to Root Certificates MUST NOT be used to sign Certificates except in the following cases:

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

CERTISIGN has implemented a combination of physical, logical, and procedural controls to ensure the security of CERTISIGN and Enterprise Customer CA private keys. Protection of CERTISIGN TRUST NETWORK Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of CERTISIGN TRUST NETWORK Private Key. CERTISIGN TRUST NETWORK encrypts its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

Subscribers are required by contract to take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of private keys.

6.2.1 Cryptographic Module Standards and Controls

Private keys within CERTISIGN TRUST NETWORK SHALL be protected using a Trustworthy System and private key holders SHALL take necessary precautions to prevent the loss, disclosure, modification, or unauthorized use of such Private Keys in accordance with this CP, contractual obligations and requirements documented in CERTISIGN TRUST NETWORK's confidential security policies. End-user Subscribers have the option of protecting their private keys in a smart card or other hardware token. CERTISIGN and enterprise RA customers SHALL protect private key segments on these servers using a Trustworthy System.

CERTISIGN TRUST NETWORK performs all CA cryptographic operations on cryptographic modules rated at a minimum of FIPS 140-1 level 3 or other similar standard used in Brazil..

CERTISIGN recommends that enterprise RA Customers perform all Automated Administration RA cryptographic operations on a cryptographic module rated at least 140-1 level 2 certified cryptographic module or other similar standard used in Brazil.

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

CERTISIGN has implemented technical and procedural mechanisms that require the participation of multiple trusted individuals to perform sensitive CA cryptographic operations. CERTISIGN uses "Secret Sharing" to split the activation data needed to make use of a CA private key into separate parts called "Secret Shares" which are held by trained and trusted individuals called "Shareholders." A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is REQUIRED to activate a CA private key stored on the module.

The threshold number of shares needed to sign a CA certificate is three (3). It SHOULD be noted that the number of shares distributed for disaster recovery tokens MAY be less than the number distributed for operational tokens, while the threshold number of REQUIRED shares remains the same. Secret Shares are protected in accordance with this CP.

6.2.3 Private Key Escrow

CA private keys are not escrowed. Escrow of private keys for end user subscribers is explained in more detail in Section 4.12.

6.2.4 Private Key Backup

CERTISIGN creates backup copies of CA private keys for routine recovery and disaster recovery purposes. Such keys are stored in encrypted form within hardware cryptographic modules and associated key storage devices. Cryptographic modules used for CA private key storage meet the requirements of this CP. CA private keys are copied to backup hardware cryptographic modules in accordance with this CP.

Modules containing onsite backup copies of CA private keys are subject to the requirements of CP. Modules containing disaster recovery copies of CA private keys are subject to the requirements of this CP.

Private keys that are backed up are to be protected from unauthorized modification or disclosure through physical or cryptographic means. Back ups are protected with a level of physical and cryptographic protection equal to or exceeding that for cryptographic modules within CERTISIGN site, such as at a disaster recovery site or at another secure off-site facility, such as a bank safe.

CERTISIGN recommends that Enterprise Customers having Automated Administration tokens who are not subject to the Certigate service back up their private keys and protect them from unauthorized modification or disclosure by physical or cryptographic means.

CERTISIGN does not store copies of others private keys.

6.2.5 Private Key Archival

Upon expiration of CERTISIGN TRUST NETWORK CA Certificate, the key pair associated with the certificate will be securely retained for a period of at least 5 years using hardware cryptographic modules that meet the requirements of this CP. These CA key pairs SHALL NOT be used for any signing events after the expiration date of the corresponding CA Certificate, unless CERTISIGN TRUST NETWORK Certificate has been renewed in terms of this CP.

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys without authorization by the Subordinate CA.

CERTISIGN does not archive copies of Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CERTISIGN generates CA key pairs on the hardware cryptographic modules in which the keys will be used. In addition, CERTISIGN makes copies of such CA key pairs for routine recovery and disaster recovery purposes. Where CA key pairs are backed up to another hardware cryptographic module, such key pairs are transported between modules in encrypted form.

If the Issuing CA generated the Private Key on behalf of the Subordinate CA, then the Issuing CA SHALL encrypt the Private Key for transport to the Subordinate CA. If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not affiliated with the Subordinate CA, then the Issuing CA SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

Entry of a private key into a cryptographic module SHALL use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

CERTISIGN TRUST NETWORK Participants pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, SHALL securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.2.7 Private Key Storage on Cryptographic Module

Entry of a private key into a cryptographic module SHALL use mechanisms to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private key.

6.2.8 Method of Activating Private Key

CERTISIGN TRUST NETWORK protects the activation data for their private keys against loss, theft, modification, unauthorized disclosure, or unauthorized use.

CERTISIGN TRUST NETWORK Standard for Subscribers Private Key protection is:

. Use a password in accordance with Section 6.4.1 or security of equivalent strength to authenticate the Subscriber before the activation of the private key, which includes, for instance, a password to operate the private key, or a Windows logon or screen saver password; and

. Take commercially reasonable measures for the physical protection of the Subscriber's workstation to prevent use of the workstation and its associated private key without the Subscriber's authorization.

When deactivated, private keys SHALL be kept in encrypted form only.

6.2.9 Method of Deactivating Private Key

CERTISIGN TRUST NETWORK CA private keys are deactivated upon removal from the token reader.

When CERTISIGN TRUST NETWORK is taken offline CERTISIGN TRUST NETWORK's personnel SHALL remove the token containing such CA's private key from the reader in order to deactivate it.

End-user Subscribers SHALL protect their private keys. Such obligations extend to protection of the private key after a private key operation has taken place. The private key MAY be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user.

End-user Subscriber private keys MAY be deactivated after each operation, upon logging off their system, or upon removal of a smart card from the smart card reader depending upon the authentication mechanism employed by the user. In all cases, end-user Subscribers have an obligation to adequately protect their private key(s) in accordance with its CPS.

6.2.10 Method of Destroying Private Key

Where required, all private keys MAY be destroyed in a manner that reasonably ensures that there are no residuals remains of the key that could lead to the reconstruction of the key.

CERTISIGN utilizes the 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.

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

CAs SHALL archive their own public keys, as well as the public keys of all CAs within their Sub-domains, in accordance Section 5.5.

CERTISIGN TRUST NETWORK CA and end-user Subscriber Certificates are backed up and archived as part of CERTISIGN 's routine backup procedures.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

The Operational Period for Certificates SHALL be set according to the time limits set forth in Table 4 below. End user Subscriber Certificates that are renewals of existing subscriber certificates MAY have a longer validity period (up to 3 months).

The usage period for end-user Subscriber key pairs is the same as the Operational Period for their Certificates, except that private keys MAY continue to be used after the Operational Period for decryption and signature verification. The Operational Period of a Certificate ends upon its expiration or revocation. A CA SHALL NOT issue

Certificates if their Operational Periods would extend beyond the usage period of the key pair of the CA. Therefore, the CA key pair usage period is necessarily shorter than the operational period of the CA Certificate. Specifically, the usage period is the Operational Period of the CA Certificate minus the Operational Period of the Certificates that the CA issues. Upon the end of the usage period for a Subscriber or CA key pair, the Subscriber or CA SHALL thereafter cease all use of the key pair, except to the extent a CA needs to sign revocation information until the end of the Operational Period of the last Certificate it has issued.

Certificate Issued By	**Validity Period**
Root CA self-signed (2048 bit RSA)	Up to 50 years
Root CA self-signed (256 bit ECC)	Up to 30 years
Root CA self-signed (384 bit ECC)	Up to 30 years
Root CA to Offline intermediate CA	Generally 10 years but up to 15 years after renewal
Root CA to online CA	Generally 5 years but up to 10 years after renewal
Offline intermediate CA to online CA	Generally 5 years but up to 10 years after renewal
Online CA to End-user Individual Subscriber	Normally up to 3 years, but under the conditions described below, up to 6 years under the conditions described below with no option to renew or re-key. After 6 years new enrollment is REQUIRED.
Online CA to End-Entity Organizational Subscriber	Normally up to 6 years30 under the conditions described below with no option to renew or re-key. After 6 years new enrollment is REQUIRED.
Online CA to SSL Certificates Subscriber	issued after 1 July 2016 but prior to 1 March 2018 MUST have a Validity Period no greater than 39 months. issued after 1 March 2018 MUST have a Validity Period no greater than 825 days.
EV Certificate	Generally 12 months. The maximum validity period SHALL NOT exceed 825 days.
Subscriber Certificates issued under CABF Requirements	issued after 1 July 2016 but prior to 1 March 2018 MUST have a Validity Period no greater than 39 months. issued after 1 March 2018 MUST have a Validity Period no greater than 825 days.
EV Code Signing Certificate	The validity period for an EV Code Signing Certificate: . issued to a Subscriber MUST NOT exceed 39 months. . issued to a Signing Authority OR a Timestamp Authority that fully complies with CABF Guidelines MUST NOT exceed 135 months.

Table 4 – Certificate Operational Periods

Except as noted in this section, CERTISIGN TRUST NETWORK Participants SHALL cease all use of their key pairs after their usage periods have expired.

Certificates issued by CAs to end-user Subscribers MAY have Operational Periods longer than three years, up to six years, if the following requirements are met:

- Protection of the Subscriber key pairs in relation to its operational environment for Organization Certificates, operation with the enhanced protection of a data center and for Individual Certificates, the Subscribers' key pairs reside on a hardware token, such as a smart card,
- Subscribers are REQUIRED to undergo re-authentication procedures at least every 3 years under CP Section 3.2.3,
- If a Subscriber is unable to complete re-authentication procedures under CP Section 3.2.3 successfully or is unable to prove possession of such private key when REQUIRED by the foregoing, the CA SHALL automatically revoke the Subscriber's Certificate.

Any exception to this procedure requires approval from the PMD and MUST be documented in the relevant CPS.

6.3.2.1 CABF Validity Period Requirements

Not applicable.

6.3.2.1.1 CABF Validity Period Requirements for EV

Not applicable.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

CERTISIGN TRUST NETWORK Participants generating and installing activation data for their private keys SHALL use methods that protect the activation data to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

To the extent passwords are used as activation data, Subscribers SHALL generate passwords that cannot easily be guessed or cracked by dictionary attacks.

Activation data (Secret Shares) used to protect tokens containing CERTISIGN TRUST NETWORK CA private keys is generated in accordance with the requirements of CPS Section 6.2.2. The creation and distribution of Secret Shares is logged.

CERTISIGN 's password selection guidelines require that passwords:

- be generated by the user;
- have at least fifteen characters;
- have at least one alphabetic and one numeric character;
- have at least one lower-case letter;
- not contain many occurrences of the same character;
- not be the same as the operator's profile name; and
- not contain a long substring of the user's profile name.

CERTISIGN strongly recommends that all Subscribers choose passwords that meet the same requirements.

CERTISIGN also recommends the use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) for private key activation.

6.4.2 Activation Data Protection

CERTISIGN TRUST NETWORK Participants SHALL protect the activation data for their private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

End-user Subscribers SHALL protect the activation data for their private keys, if any, to the extent necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

CERTISIGN TRUST NETWORK utilizes Secret Sharing in accordance with its CPS, this CP and the standards documented in CERTISIGN TRUST NETWORK's confidential security policies. CERTISIGN TRUST NETWORK provides the procedures and means to enable Shareholders to take the precautions necessary to prevent the loss, theft, modification, unauthorized disclosure, or unauthorized use of the Secret Shares thatthey possess. Shareholders SHALL NOT:

- Copy, disclose, or make the Secret Share available to a third party, or make any unauthorized use of it whatsoever; or
- disclose his, her, or any other person's status as a Shareholder to any third party.

The Secret Shares and any information disclosed to the Shareholder in connection with his or her duties as a Shareholder constitute Confidential/Private Information.

CERTISIGN Shareholders are REQUIRED to safeguard their Secret Shares and sign an agreement acknowledging their Shareholder responsibilities.

CERTISIGN strongly recommends that all Subscribers store their private keys in encrypted form and protect their private keys through the use of a hardwaretoken and/or strong passphrase. The use of two factor authentication mechanisms (e.g., token and passphrase, biometric and token, or biometric and passphrase) is encouraged.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation Data Transmission

When activation data for their private keys are transmitted, CERTISIGN TRUST NETWORK Participants SHALL protect the transmission using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

6.4.3.2 Activation Data Destruction

Activation data for CA private keys SHALL be decommissioned using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of the private keys protected by such activation data. After the record retention periods in CPS Section 5.5.2 lapses, CERTISIGN TRUST NETWORK SHALL decommission activation data by overwriting and/or physical destruction.

6.5 Computer Security Controls

CA and RA functions take place on Trustworthy Systems in accordance with the standards documented in CERTISIGN TRUST NETWORK's confidential security policies.

6.5.1 Specific Computer Security Technical Requirements

CERTISIGN ensures that the systems maintaining CA software and data files are Trustworthy Systems secure from unauthorized access. In addition, CERTISIGN limits access to production servers to those individuals with a valid business reason for such access. General application users do not have accounts on production servers.

CERTISIGN 's production network is logically separated from other components. This separation prevents network access except through defined application processes. CERTISIGN uses firewalls to protect the production network from internal and external intrusion and limit the nature and source of network activities that MAY access production systems.

CERTISIGN requires the use of passwords that have a minimum character length and a combination of alphanumeric and special characters. CERTISIGN requires that passwords be changed on a periodic basis.

Direct access to CERTISIGN databases supporting CERTISIGN 's CA Operations is limited to Trusted Persons in CERTISIGN 's Production Operations group having a valid business reason for such access.

CERTISIGN enforces multi-factor authentication for all accounts capable of directly causing certificate issuance.

Gateway servers SHALL include the following functionality: access control to CA services, identification and authentication for launching of CA services, object re-use for CA random access memory, use of cryptography for session communication and database security, archival of CA and end-user Subscriber history and audit data, audit of security related events, self-test of security related CA services, and Trusted path for identification of PKI roles and associated identities.

RAs SHALL ensure that the systems maintaining RA software and data files are Trustworthy Systems secure from unauthorized access, which can be demonstrated by compliance with audit criteria applicable under CPS Section 5.4.1.

RAs SHALL logically separate access to these systems and this information from other components. This separation prevents access except through defined processes. RAs SHALL use firewalls to protect the network from internal and external intrusion and limit the nature and source of activities that MAY access such systems and information. RAs SHALL require the use of passwords with a minimum character length and a combination of alphanumeric and special characters, and SHALL require that passwords be changed on a periodic basis and as necessary. Direct access to the RA's database maintaining Subscriber information SHALL be limited to Trusted Persons in the RA's operations group having a valid business reason for such access.

6.5.1.1 CABF Requirements for System Security

CERTISIGN TRUST NETWORK SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.1.1.1 CABF Requirements for System Security for EV

Not applicable.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Technical Controls

6.6.1 System Development Controls

Applications are developed and implemented by CERTISIGN in accordance with CERTISIGN systems development and change management standards. CERTISIGN also provides software to its Enterprise Customers for performing RA and certain CA functions. Such software is developed in accordance with CERTISIGN system development standards.

CERTISIGN developed software, when first loaded, provides a method to verify that the software on the system originated from CERTISIGN, has not been modified prior to installation, and is the version intended for use.

6.6.2 Security Management Controls

CERTISIGN has mechanisms and/or policies in place to control and monitor the configuration of its CA systems. CERTISIGN validates the integrity of its CA systems.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

CA and RA functions are performed using networks secured in accordance with the standards documented in CERTISIGN TRUST NETWORK's confidential security policies (in the case of CERTISIGN and Affiliates) to prevent unauthorized access, tampering, and denial-of-service attacks. Communications of sensitive information SHALL be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

6.8 Time-Stamping

Certificates, CRLs, and other revocation database entries SHALL contain time and date information.

7. Certificate, CRL and OCSP Profiles

All Certificates and Certificate Revocation Lists SHALL comply with RFC 5280 and RFC 6818. They SHALL additionally comply with RFC3279, RFC4055, RFC5480, RFC5756, RFC5758 as appropriate based on the Subject Public Key Info and the Signature Algorithm present in the certificate.

7.1 Certificate Profile

CERTISIGN TRUST NETWORK Certificates generally conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 5280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 5280").

As applicable to the Certificate type, CERTISIGN TRUST NETWORK Certificates conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

At a minimum, X.509 CERTISIGN TRUST NETWORK Certificates SHALL contain the basic fields and indicated prescribed values or value constraints in Table below:

Field	Value or Value constraint
Serial Number	Unique value per Issuer DN that exhibits at least 20 bits of entropy and greater than zero containing at least 64 bits of output from a CSPRNG
Signature Algorithm	Object identifier of the algorithm used to sign the certificate (See Section 7.1.3)
Issuer DN	See Section 7.1.4
Valid From	Universal Coordinate Time base. Synchronized to Master Clock of Brazilian Observatory. Encoded in accordance with RFC 5280.
Valid To	
Subject DN	See Section 7.1.4
Subject Public Key	Encoded in accordance with RFC 5280
Signature	Generated and encoded in accordance with RFC 5280

Table 5- Certificate Profile Basic Fields

7.1.1 Version Number(s)

CERTISIGN CA Certificates and End-user Subscriber Certificates are of type X.509 Version 3 Certificates.

7.1.2 Certificate Extensions

CERTISIGN SHALL populate X.509 Version 3 CERTISIGN TRUST NETWORK Certificates with the extensions required by this Section.

basicConstraints

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional	required	required	optional
criticality field	MUST be set TRUE	MUST be set TRUE	Must not be TRUE
pathLenConstraint field	SHOULD NOT be present	MAY be present. Shall have the extension set to the maximum number of CA certificates that MAY follow this Certificate in a certification path. CA Certificates issuing end-user Subscriber Certificates SHALL have the field set to a value of "0" indicating that only an end-user Subscriber Certificate MAY follow in the certification path.	--
cA field		MUST be present	

Table 6 -basicConstraints

keyUsage

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional	required	required	optional
criticality field	MUST be set TRUE	MUST be set TRUE	Should be set TRUE or

			FALSE
bit positions for keyCertSign and cRLSign	They MUST be set	They MUST be set	If present, they MUST NOT be set
bit positions for digitalSignature	If CA is used for signing OCSP responses, then it MUST be set	If CA is used for signing OCSP responses, then it MUST be set	--

Table 7 - keyUsage

certificatePolicies

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional	SHOULD NOT be present	required	required
criticality field	SHALL be set to FALSE	SHALL be set to FALSE	SHALL be set to FALSE
certificatePolicies:policyIdentifier - Required/Optional	--	required	required
certificatePolicies:policyQualifiers - contents	--	The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA. certificatePolicies:policyQualifiers:policyQualifierId (Optional) . id-qt 1 [RFC 5280]. certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional) . HTTP URL for the Root CA's CP, CPS, Relying Party Agreement, or other pointer to online policy information provided by the CA.	The following extensions MAY be present: certificatePolicies:policyQualifiers:policyQualifierId (Recommended) . id-qt 1 [RFC 5280]. certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional) . HTTP URL for the Subordinate CA's CPS, Relying Party Agreement or other pointer to online information provided by the CA

Table 8 - certificatePolicies

ExtendedKeyUsage[7]

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional	MUST NOT be present	optional	required
criticality field	--	If present, SHOULD set FALSE	Must be set FALSE
content		. Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] MUST be present. . Other values MAY be present.	. Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] MUST be present. . id-kp-emailProtection [RFC5280] MAY be

[7] Generally Extended Key Usage will only appear within end entity certificates (as highlighted in RFC 5280 (4.2.1.12)), however, Subordinate CAs MAY include the extension to further protect relying parties until the use of the extension is consistent between Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.

			present. . Other values SHOULD NOT be present.

Table 9 - ExtendedKeyUsage

cRLDistributionPoints

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional		required	MAY be present
criticality field	--	Must be set FALSE	. If present, MUST be set FALSE
content	--	It MUST contain the HTTP URL of the CA's CRL service.	it MUST contain the HTTP URL of the CA's CRL service.

Table 10 - cRLDistributionPoints

authorityInformationAccess

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional		required, with the exception of stapling, which is noted below	required, with the exception of stapling, which is noted below
criticality field		Must be set FALSE	Must be set FALSE
content		. It MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod=1.3.6.1.5.5.7.48.1). . It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod=1.3.6.1.5.5.7.48.2). . The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].	. It MUST contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod=1.3.6.1.5.5.7.48.1). . It SHOULD also contain the HTTP URL of the Issuing CA's certificate (accessMethod=1.3.6.1.5.5.7.48.2). . The HTTP URL of the Issuing CA's OCSP responder MAY be omitted provided that the Subscriber "staples" OCSP responses for the Certificate in its TLS handshakes [RFC4366].

Table 11 - authorityInformationAccess

Subject Key Identifier

Type of Certificate	Root CA	Subordinate CA	Subscriber
criticality field		If present, SHOULD be set FALSE	If present, SHOULD be set FALSE

Table 12 - Subject Key Identifier

nameConstraints [8]

Type of Certificate	Root CA	Subordinate CA	Subscriber
Required/Optional	--	Optional	--
criticality field	--	If present, SHOULD be set TRUE	--

Table 23 - nameConstraints

All other fields and extensions MUST be set in accordance with RFC 5280. CERTISIGN TRUST NETWORK will not issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified above unless CERTISIGN TRUST NETWORK is aware of a reason for including the data in the Certificate.

CERTISIGN TRUST NETWORK will not issue a Certificate with:
a. Extensions that do not apply in the context of the public Internet[9] unless:
i. such value falls within an OID arc for which the Applicant demonstrates ownership, or
ii. the Applicant can otherwise demonstrate the right to assert the data in a public context; or
b. semantics that, if included, will mislead a Relying Party about the certificate information verified by CERTISIGN TRUST NETWORK[10].

7.1.2.1 Subject Alternative Names

The subjectAltName extension of X.509 Version 3 Certificates are populated in accordance with RFC 5280.

The criticality field of this extension SHALL be set to FALSE.

7.1.2.2 CABF Requirement for Certificate Policies Extension

Not applicable.

7.1.2.3 CABF Requirement for Certificate Policies Extension for EV

All provisions of Section 7.1.2 related with Certificate Extensions apply to EV Certificates with the following exceptions:

1) If a Subordinate CA Certificates is issued to a Subordinate CA not controlled by the entity that controls the Root CA, the policy identifiers in the certificatePolicies extension MUST include the CA's Extended Validation policy identifier.
Otherwise, it MAY contain the anyPolicy identifier.

2) The following fields MUST be present if the Subordinate CA is not controlled by the entity that controls the Root CA.

certificatePolicies:policyQualifiers:policyQualifierId
id-qt 1 [RFC 5280]

certificatePolicies:policyQualifiers:qualifier:cPSuri
HTTP URL for the Root CA's Certification Practice Statement

3) The certificatePolicies extension in EV Certificates issued to Subscribers MUST include the following:
certificatePolicies:policyIdentifier (Required)
The Issuer's EV policy identifier

certificatePolicies:policyQualifiers:policyQualifierId (Required)
id-qt 1 [RFC 5280]

[8] Non-critical Name Constraints are an exception to RFC 5280 (4.2.1.10), however, they MAY be used until the Name Constraints extension is supported by Application Software Suppliers whose software is used by a substantial portion of Relying Parties worldwide.
[9] such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network
[10] such as including extendedKeyUsage value for a smart card, where CERTISIGN AC PARCERIA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance

certificatePolicies:policyQualifiers:qualifier:cPSuri (Required)
HTTP URL for the Subordinate CA's Certification Practice Statement

4) The cRLDistribution Point extension MUST be present in Subscriber Certificates if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension.

7.1.2.4 CABF Requirement for Certificate Policies Extension for EV Code Signing Certificates

All provisions of Section 7.1.2.3 related with Certificate Extensions apply to EV Code Signing Certificates with the following exceptions:
1) the Domain Name SHALL be omitted;

2) the keyUsage extension MUST be set as follows:
This extension MUST be present and MUST be marked critical.
The bit position for digitalSignature MUST be set.
All other bit positions SHOULD NOT be set;

AND
3) the extended keyUsage extension MUST be set as follows:
This extension MUST be present, and the value id-kp-codeSigning MUST be present.
Other values SHOULD NOT be present.

7.1.2.5. Application of RFC 5280

For purposes of clarification, a Precertificate, as described in RFC 6962 – Certificate Transparency, shall not be considered to be a "certificate" subject to the requirements of RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile under these Policies.

7.1.3 Algorithm Object Identifiers

CERTISIGN TRUST NETWORK Certificates are signed using one of following algorithms:

- sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
- ecdsa-with-Sha256 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2}
- ecdsa-with-Sha384 OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3}

Certificate signatures produced using these algorithms SHALL comply with RFC 3279.

7.1.3.1 CABF Algorithm Object Identifiers Requirements

- CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm.
- This Section does not apply to Root CA or CA cross certificates.
- CAs MAY continue to use their existing SHA-1 Root Certificates.
- SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1 Subordinate CA Certificate.

7.1.4 Name Forms

CERTISIGN TRUST NETWORK Certificates are populated with the Issuer Name and Subject Distinguished Name required under CPS Section 3.1.1.

In addition, end-user Subscriber Certificates generally include an additional Organizational Unit field that contains a notice stating that the terms of use of the Certificate are set forth in a URL, and the URL SHALL be a pointer to the applicable Relying Party Agreement. Exceptions to the foregoing requirement SHALL be permitted when space, formatting, or interoperability limitations within Certificates make such an Organizational Unit impossible

to use in conjunction with the application for which the Certificates are intended, or if a pointer to the applicable Relying Party Agreement is included in the policy extension of the certificate.

7.1.4.1. Issuer Information

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

7.1.4.1.1. CABF Issuer Information Requirements for EV Certificate

Issuer Information listed in an EV Certificate MUST comply with Section 7.1.4.1 of the Baseline Requirements.

7.1.4.2. Subject Information – Subscriber Certificates

By issuing the Certificate, CERTISIGN TRUST NETWORK represents that it followed the procedure set forth in this CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

For SSL Certificates, CERTISIGN TRUST NETWORK will not include a Domain Name or IP Address in a Subject atribute.

7.1.4.2.1. CABF Subject Alternative Name Extension Requirements

Certificate Field: extensions:subjectAltName
Required/Optional: Required
Contents:

- The subjectAlternativeName extension is REQUIRED and contains at least one entry.
- In SSL Certificates, each entry is either a dNSName containing the FQDN or an iPAddress containing the IP address of a server.
- CERTISIGN TRUST NETWORK confirms that the Applicant controls the FQDN or IP address or has been granted the right to use it by the Domain Name Registrant or IP address assignee, as appropriate.
- Wildcard FQDNs are permitted.

Prior to April 1, 2019, certificates containing underscore characters ("_") in domain labels in dNSName entries MAY be issued as follows:
• dNSName entries MAY include underscore characters such that replacing all underscore characters with hyphen characters ("-") would result in a valid domain label, and;
• Underscore characters MUST NOT be placed in the left most domain label, and;
• Such certificates MUST NOT be valid for longer than 30 days.

All certificates containing an underscore character in any dNSName entry and having a validity period of more than 30 days MUST be revoked prior to January 15, 2019.
- After April 30, 2019, underscore characters ("_") MUST NOT be present in dNSName entries.

7.1.4.2.1.1. Reserved IP Address or Internal Name

CERTISIGN TRUST NETWORK SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice was eliminated by October 2016 and won´t issue a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name.

7.1.4.2.2. CABF Subject Distinguished Name Fields Requirements

a. Certificate Field: subject:commonName (OID 2.5.4.3)
Required/Optional: Deprecated (Discouraged, but not prohibited)
Contents: If present, commonName MUST contains a FQDN Name that is also one of the values contained in the Certificate's subjectAlternativeName extension.

b. Certificate Field: subject:organizationName (OID 2.5.4.10)

Required/Optional: Required.
Contents:

- It MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

- If the Subject is a natural person, because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey the Subject's name or DBA (see CP section 3.2.2.1).

- If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA SHALL document the discrepancy and SHALL use locally accepted abbreviations when abbreviating the organization name (e.g., if the official record shows "Company Name Incorporated", the CA MAY include "Company Name, Inc.").

c. Certificate Field: subject:givenName (2.5.4.42) and subject:surname (2.5.4.4)
Required/Optional: Optional.
Contents:

- If present, the subject:givenName field and subject:surname field MUST contain an natural person Subject's name as verified under Section 3.2.3.
- A Certificate containing a subject:givenName field or subject:surname field MUST contain the (2.23.140.1.2.3) CP OID.

d. Certificate Field: Number and street: subject:streetAddress (OID: 2.5.4.9)
Required/Optional:
. Optional if the subject:organizationName field, subject: givenName field, or subject:surname field are present.
. Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent.
Contents: If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 3.2.2.1.

e. Certificate Field: subject:localityName (OID: 2.5.4.7)
Required/Optional:
. Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and the subject:stateOrProvinceName field is absent.
. Optional if the subject:stateOrProvinceName field and the subject:organizationName field, subject:givenName field, or subject:surname field are present.
. Prohibited if the subject:organizationName field, subject:givenName, and subject:surname field are absent.
Contents: If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the localityName field MAY contain the Subject's locality and/or state or province information as verified under Section 3.2.2.1.

f. Certificate Field: subject:stateOrProvinceName (OID: 2.5.4.8)
Required/Optional:
. Required if the subject:organizationName field, subject:givenName field, or subject:surname field are present and subject:localityName field is absent.
. Optional if the subject:localityName field and the subject:organizationName field, and subject:givenName field , or subject:surname field are present.
. Prohibited if the subject:organizationName field, subject:givenName field , or subject:surname field are absent.
Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 3.2.2.1. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 7.1.4.2.2(g), the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 3.2.2.1.

g. Certificate Field: subject:postalCode (OID: 2.5.4.17)
Required/Optional:
. Optional if the subject:organizationName, subject:givenName field, or subject:surname fields are present.
. Prohibited if the subject:organizationName field, subject:givenName field, or subject:surname field are absent.
Contents: If present, the subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 3.2.2.1.

h. Certificate Field: subject:countryName (OID: 2.5.4.6)
Required/Optional:
. Required if the subject:organizationName field, subject:givenName, or subject:surname field are present.
. Optional if the subject:organizationName field, subject:givenName field, and subject:surname field are absent.
Contents:
. If the subject:organizationName field is present, the subject:countryName MUST contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.2.1.
. If the subject:organizationName field is absent, the subject:countryName MAY contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 3.2.2.3.
. If a Country is not represented by an official ISO 3166-1 country code, CERTISIGN TRUST NETWORK MAY specify the ISO 3166-1 user-assigned code of XX indicating that an official ISO 3166-1 alpha-2 code has not been assigned.

i. Certificate Field: subject:organizationalUnitName
Required/Optional: Optional.
- The CA implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information in accordance with CP section 3.2.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with CP section 3.2.2.

j. Other Subject Attributes
- Optional attributes, when present in the subject field, MUST contain information that has been verified by the CA. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, MUST NOT be used.

7.1.4.2.3. Subject Distinguished Name Fields for EV Certificates

a. Certificate Field: subject: organizationName (OID 2.5.4.10)
Required/Optional: Required
Contents:
- This field MUST contain the 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 the CA as provided herein.

- If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA SHALL document the discrepancy and SHALL use locally accepted abbreviations when abbreviating the organization name (e.g., if the official record shows "Company Name Incorporated", the CA MAY include "Company Name, Inc."). The organizationName field MAY include a verified DBA or tradename of the Subject.

- When abbreviating a Subject's full legal name as allowed by this subsection, CERTISIGN TRUST NETWORK MUST use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration.

- In addition, an assumed name or DBA name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis.

- If the combination of names or the organization name by itself exceeds 64 characters, CERTISIGN TRUST NETWORK MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that CERTISIGN TRUST NETWORK checks this field in accordance with Appendix C, Item 12.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, CERTISIGN TRUST NETWORK MUST NOT issue the EV Certificate.

b. Certificate Field: subject:commonName (OID: 2.5.4.3)
Required/Optional: Deprecated (Discouraged, but not prohibited)
Contents: If present, this field MUST contain a single Domain Name owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).

Wildcard certificates are not allowed for EV Certificates except as permitted under Appendix I.

c. Certificate Field: subject:businessCategory (OID: 2.5.4.15)
Required/Optional: Required
Contents: This field MUST contain one of the following strings: "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of CPS Section 1.4.1.4.1

d. Certificate Fields:
Locality (if required):
subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)

State or province (if required):
subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)

Country:
subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)

Required/Optional: Required
Contents: These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information.
Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction.

e. Certificate Field: subject: serialNumber (OID: 2.5.4.5)
Required/Optional: Required
Contents: For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats.
For Government Entities that do not have a Registration Number or readily verifiable date of creation, CERTISIGN TRUST NETWORK SHALL enter appropriate language to indicate that the Subject is a Government Entity.
For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.

f. Certificate Fields:
Number and street:
subject:streetAddress (OID: 2.5.4.9)
City or town:
subject:localityName (OID: 2.5.4.7)
State or province (where applicable):
subject:stateOrProvinceName (OID: 2.5.4.8)
Country:
subject:countryName (OID: 2.5.4.6)
Postal code:
subject:postalCode (OID: 2.5.4.17)
Required/Optional: As stated in Section 7.1.4.2.2.

Contents: This field MUST contain the address of the physical location of the Subject's Place of Business.

g. Other Subject Attributes
- All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. The CA SHALL NOT include FQDN in Subject atributes.
- Optional attributes, when present in the subject field, MUST contain information that has been verified by the CA or MUST be left empty. Metadata such as '.', '-', and ' ' (i.e. space) characters, and/or any other indication that the value is absent, incomplete, or not applicable, MUST NOT be used.

7.1.4.2.4. Subject Alternative Name Extension for EV Certificates

a. Certificate Field: subject: subjectAltName:dNSName
Required/Optional: Required
Contents:
- This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service).

- Wildcard certificates are not allowed for EV Certificates.

7.1.4.2.5. Subject Distinguished Name Fields for EV Code Signing Certificates

a. Certificate Field: subject: organizationName (OID 2.5.4.10): as described in 7.1.4.2.3. a.

b. Certificate Field: subject:businessCategory (OID: 2.5.4.15)
As described in 7.1.4.2.3.c.

c. Certificate Fields:
Locality (if required):
subject:jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)
ASN.1 - X520LocalityName as specified in RFC 5280
State or province (if required):
subject:jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)
ASN.1 - X520StateOrProvinceName as specified in RFC 5280
Country:
subject:jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)
ASN.1 – X520countryName as specified in RFC 5280
As described in 7.1.4.2.3.d.

d. Certificate Field: subject: serialNumber (OID: 2.5.4.5)
As described in 7.1.4.2.3.e.

e. Certificate Fields:
Number and street:
subject:streetAddress (OID: 2.5.4.9)
City or town:
subject:localityName (OID: 2.5.4.7)
State or province (where applicable):
subject:stateOrProvinceName (OID: 2.5.4.8)
Country:
subject:countryName (OID: 2.5.4.6)
Postal code:
subject:postalCode (OID: 2.5.4.17)
As described in 7.1.4.2.3.f.

f. Other Subject Attributes
As described in 7.1.4.2.3.g.

7.1.4.2.6. Subject Alternative Name Extension for EV Code Signing Certificates

No stipulation.

7.1.4.3. Subject Information – Root Certificates and Subordinate CA Certificates

By issuing a Subordinate CA Certificate, CERTISIGN TRUST NETWORK represents that it followed the procedure set forth in this CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1. Subject Distinguished Name Fields

a. Certificate Field: subject:commonName (OID 2.5.4.3)
Required/Optional: Required
Contents: This field MUST be present and the contents SHOULD be an identifier for the certificate such that the certificate's Name is unique across all certificates issued by the issuing certificate.

b. Certificate Field: subject:organizationName (OID 2.5.4.10)
Required/Optional: Required.
Contents:

- It MUST contain either the Subject CA's name or DBA as verified under Section 3.2.2.2.

- If the Subject is a natural person, because Subject name attributes for individuals (e.g. givenName (2.5.4.42) and surname (2.5.4.4)) are not broadly supported by application software, the CA MAY use the subject:organizationName field to convey the Subject's name or DBA (see CP section 3.2.2.1).

- If the fields include discrepancies that the CA considers minor, such as common variations and abbreviations, then the CA SHALL document the discrepancy and SHALL use locally accepted abbreviations when abbreviating the organization name (e.g., if the official record shows "Company Name Incorporated", the CA MAY include "Company Name, Inc.").

c. Certificate Field: subject:countryName (OID: 2.5.4.6)
Required/Optional: Required
Contents: This field MUST contain the two-letter ISO 3166-1 country code for the country in which the CA place of business is located.

7.1.5 Name Constraints

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate MUST include an Extended Key Usage (EKU) extension specifying all extended key usages that the Subordinate CA Certificate is authorized to issue certificates for. The anyExtendedKeyUsage KeyPurposeId MUST NOT appear within this extension.

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:
(a) For each dNSName in permittedSubtrees, CERTISIGN TRUST NETWORK MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of section 3.2.2.4.
(b) For each iPAddress range in permittedSubtrees, CERTISIGN TRUST NETWORK MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf.
(c) For each DirectoryName in permittedSubtrees CERTISIGN TRUST NETWORK MUST confirm the Applicants and/or Subsidiary's Organizational name and location such that end entity certificates issued from the subordinate CA Certificate will be in compliancy with section 7.1.2.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate MUST specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate MUST include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4

address range of 0.0.0.0/0). The Subordinate CA Certificate MUST also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0).
Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

If the Subordinate CA is not allowed to issue certificates with dNSNames, then the Subordinate CA Certificate MUST include a zero-length dNSName in excludedSubtrees. Otherwise, the Subordinate CA Certificate MUST include at least one dNSName in permittedSubtrees.

7.1.6 Certificate Policy Object Identifier

Where the Certificate Policies extension is used, Certificates contain the object identifier for the Certificate Policy corresponding to the appropriate type of Certificate as set forth in Section1.2. For legacy Certificates issued prior to the publication of CERTISIGN TRUST NETWORK CP which include the Certificate Policies extension, Certificates refer to CERTISIGN TRUST NETWORK CPS.

7.1.6.1. Reserved CP Identifiers

Not applicable.

7.1.6.2. Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

7.1.6.3. Subordinate CA Certificates

A Certificate issued to a Subordinate CA that is not an Affiliate of the Issuing CA:

1. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers or identifiers defined by CERTISIGN TRUST NETWORK in this CP and/or CPS) and
2. MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0).

A Certificate issued to a Subordinate CA that is an affiliate of the Issuing CA:

1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by CERTISIGN TRUST NETWORK in this CP and/or CPS to indicate the Subordinate CA's compliance with these Requirements and
2. MAY contain the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier.

A Subordinate CA SHALL represent, in this CP and/or CPS, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

7.1.6.4. Subscriber Certificates

A Certificate issued to a Subscriber MUST contain one or more policy identifier(s), defined by the Issuing CA, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with these Requirements. CAs complying with these Requirements MAY also assert one of the reserved policy OIDs in such Certificates.

The issuing CA SHALL document in this CP or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

7.1.6.5 CABF Requirements for CP Object Identifier

7.1.6.5.1 CABF Requirements for CP Object Identifier for EV

Not applicable.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

CERTISIGN generally populates X.509 Version 3 CERTISIGN TRUST NETWORK Certificates with a policy qualifier within the Certificate Policies extension. Generally, such Certificates contain a CPS pointer qualifier that points to

the applicable Relying Party Agreement or CERTISIGN TRUST NETWORK CPS. In addition, some Certificates contain a User Notice Qualifier which points to the applicable Relying Party Agreement.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2 CRL Profile

As applicable to the Certificate type, corresponding CRLs conform to the current version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

Version 2 CRLs conform to RFC 5280 and contain the basic fields and contents specified in Table below:

Field	Value or Value constraint
Version	See Section 7.2.1.
Signature Algorithm	Algorithm used to sign the CRL in accordance with RFC 3279. (See Section 7.1.3)
Issuer	Entity who has signed and issued the CRL
Effective Date	Issue date of the CRL. CRLs are effective upon issuance.
Next Update	Date by which the next CRL will be issued. CRL issuance frequency is in accordance with the requirements of Section 4.9.7
Revoked Certificates	Listing of revoked certificates, including the Serial Number of the revoked Certificate and the Revocation Date

Table 14 - CRL Profile Basic Fields

7.2.1 Version Number(s)

CERTISIGN supports both X.509 Version1 and Version 2 CRLs. Version 2 CRLs comply with the requirements of RFC 5280.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

7.3 OCSP Profile

OCSP (Online Certificate Status Protocol) is a way to obtain timely information about the revocation status of a particular certificate.

Domain validated and organization validated SSL Certificates conform to CERTISIGN TRUST NETWORK / Browser Forum Baseline requirements.

OCSP Responses SHALL conform to RFC5019 and either be:

- Signed by CERTISIGN TRUST NETWORK that issued the Certificates whose revocation status is being checked, or
- Signed by an OCSP Responder whose Certificate is signed by CERTISIGN TRUST NETWORK that issued the Certificate whose revocation status is being checked. Such OCSP Responder signing Certificate SHALL contain the extension id-pkix-ocsp-nocheck as defined by RFC6960.

7.3.1 Version Number(s)

Version 1 of the OCSP specification as defined by RFC6960 and Version 1 of the OCSP specification as defined by RFC 5019 are supported.

7.3.2 OCSP Extensions

CERTISIGN Service uses secure timestamp and validity period to establish the current freshness of each OCSP response. CERTISIGN does not use a nonce to establish the current freshness of each OCSP response and clients

SHOULD NOT expect a nonce in the response to a request that contains a nonce. Instead, clients SHOULD use the local clock to check for response freshness.

7.3.3 CABF Requirement for OCSP Signing for EV

Not applicable.

8. Compliance Audit and Other Assessments

CERTISIGN and Affiliates undergo a periodic compliance audit ("Compliance Audit") to ensure compliance with CERTISIGN TRUST NETWORK Standards after they begin operations.

An annual WebTrust for Certification Authorities v2.0 or later (or equivalent) examination is performed for Certisign's data center operations and key management operations supporting Certisign's public and Managed PKI CA services including the STN Root CAs.

In addition to these compliance audits, CERTISIGN and Affiliates SHALL be entitled to perform other reviews and investigations to ensure the trustworthiness of CERTISIGN TRUST NETWORK, which include, but are not limited to:

- A "Security and Practices Review" of an Affiliate before it is permitted to begin operations.
- A Security and Practices Review consists of a review of an Affiliate's secure facility, security documents, CPS, CERTISIGN TRUST NETWORK-related agreements, privacy policy, and validation plans to ensure that the Affiliate meets CERTISIGN TRUST NETWORK Standards.
- CERTISIGN SHALL be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself, an Affiliate, or an Enterprise Customer in the event CERTISIGN or the Superior Entity of the entity to be audited has reason to believe that the audited entity has failed to meet CERTISIGN TRUST NETWORK Standards, has experienced an incident or compromise, or has acted or failed to act, such that the audited entity's failure, the incident or compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of CERTISIGN TRUST NETWORK.
- CERTISIGN SHALL be entitled to perform "Supplemental Risk Management Reviews" on itself, an Affiliate, or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business.

CERTISIGN SHALL be entitled to delegate the performance of these audits, reviews, and investigations to the Superior Entity of the entity being audited, reviewed, or investigated or to a third party audit firm. Entities that are subject to an audit, review, or investigation SHALL provide reasonable cooperation with CERTISIGN and the personnel performing the audit, review, or investigation.

CERTISIGN TRUST NETWORK SHALL at all times:
1. Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
2. Comply with these Requirements;
3. Comply with the audit requirements set forth in this section; and
4. Be licensed as a CA in each jurisdiction where it operates, if licensing is REQUIRED by the law of such jurisdiction for the issuance of Certificates.

CABF Requirement for Audits

Not applicable.

CABF Requirement for Audits for EV

Eligible Audit Schemes

An Issuer issuing EV Certificates and EV Code Signing Objects SHALL undergo an audit in accordance with one of the following schemes:

(i) WebTrust Program for CAs audit and WebTrust EV Program audit, or
(ii) ETSI TS 102 042 audit for EVCP.

Additionaly, an Issuer issuing EV Certificates SHALL undergo an audit in accordance with
ETSI EN 319 411-1 audit for EVCP policy.

Note: If the Issuer is a Government Entity, an audit of the Issuer by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government CA has successfully passed the audit.

EV audits MUST cover all Issuer obligations under this CPS regardless of whether they are performed directly by Issuer or delegated to an RA or subcontractor.

Pre-Issuance Readiness Audit

(1) If the CA has a currently valid WebTrust Seal of Assurance for CAs, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.
(2) If the CA has a currently valid ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI TS 102 042.
(3) If the CA has a currently valid ETSI EN 319 411-1 audit for EVCP policy, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI EN 319 411-1 for EVCP.
(4) If the CA does not have a currently valid WebTrust Seal of Assurance for CAs or an ETSI 102 042 EVCP audit or an ETSI EN 319 411-1 audit for EVCP policy, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete either: (i) a point-in-time readiness assessment audit against the WebTrust for CA Program, or (ii) a point-in-time readiness assessment audit against the WebTrust EV Program, the ETSI TS 102 042 EVCP, or the ETSI EN 319 411-1 for EVCP policy.

The CA MUST complete any required point-in-time readiness assessment no earlier than 12 months prior to issuing an EV Certificate. The CA MUST undergo a complete audit under such scheme within 90 days of issuing the first EV Certificate.

8.1 Frequency and Circumstances of Assessment

Compliance Audits are conducted at least annually at the sole expense of the audited entity. Audits SHALL be conducted over unbroken sequences of audit periods with each period no longer than one year duration.

Certificates that are capable of being used to issue new certificates MUST either be :
. Technically Constrained in line With CP section 7.1.5 and audited in line with section 8.7 only, or
. Unconstrained and fully audited in line with all remaining requirements from this section.

A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with CERTISIGN TRUST NETWORK boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

(1) If CERTISIGN TRUST NETWORK has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1, then no pre-issuance readiness assessment is necessary.
(2) If CERTISIGN TRUST NETWORK does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then, before issuing Publicly-Trusted Certificates, CERTISIGN TRUST

NETWORK SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.1. The point-in-time readiness assessment SHALL be completed no earlier than 12 months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within 90 days of issuing the first Publicly-Trusted Certificate.

8.2 Identity/Qualifications of Assessor

CERTISIGN TRUST NETWORK audit SHALL be performed by a Qualified Auditor.
A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills:
1. Independence from the subject of the audit;
2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1);
3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ISSO 17065 applying the requirements specified in ETSI EN 319 403;
5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust;
6. Bound by law, government regulation, or professional code of ethics; and
7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's Relationship to Assessed Entity

Compliance audits of CERTISIGN's operations are performed by a public accounting firm that is independent of CERTISIGN.

8.4 Topics Covered by Assessment

CERTISIGN TRUST NETWORK SHALL undergo an audit in accordance with one of the following schemes:
1. "WebTrust for CAs v2.0 or newer" AND "WebTrust for CAs SSL Baseline with Network Security v2.2 or newer"; or
2. ETSI EN 319 411-1, which includes normative references to ETSI EN 319 401 (the latest version of the referenced ETSI documents should be applied); or
3. If a Government CA is REQUIRED by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

Whichever scheme is chosen, it MUST incorporate periodic monitoring and/or accountability procedures to ensure that its audits continue to be conducted in accordance with the requirements of the scheme.

The audit MUST be conducted by a Qualified Auditor.

For Delegated Third Parties which are not Enterprise RAs, CERTISIGN TRUST NETWORK SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.1, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or CERTISIGN TRUST NETWORK CP and/or CPS. If the opinion is that the Delegated Third Party does not comply, then CERTISIGN TRUST NETWORK SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with CERTISIGN TRUST NETWORK audit). However, if CERTISIGN TRUST NETWORK or Delegated Third Party is under the

operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are REQUIRED to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case MAY any non-core control be audited less often than once every three years.

8.4.1. Audits of RAs

It is RECOMMENDED that Enterprise Customers authorizing the issuance of SSL certificates undergo an annual compliance audit of their obligations under CERTISIGN TRUST NETWORK. Upon request from CERTISIGN and/or a Superior Entity (if the Superior Entity is not CERTISIGN) Enterprise Customers SHALL undergo an audit noting any exceptions or irregularities to CERTISIGN TRUST NETWORK policies and the steps taken to remedy the irregularities.

8.4.2. Audit of CERTISIGN or an Affiliate

CERTISIGN and each Affiliate SHALL be audited pursuant to the guidelines provided in the American Institute of Certificate Public Accounts' Statement on Service Organizations Control (SOC) Reports on the risks associated with Service Organizations. Their Compliance Audits SHALL be a WebTrust for Certification Authorities or an equivalent audit standard approved by CERTISIGN which includes: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.

8.5 Actions Taken as a Result of Deficiency

After receiving a Compliance Audit report, the audited entity's Superior Entity SHALL contact the audited party to discuss any exceptions or deficiencies shown by the Compliance Audit. CERTISIGN SHALL also be entitled to discuss such exceptions or deficiencies with the audited party. The audited entity and the Superior Entity SHALL, in good faith, use commercially reasonable efforts to agree on a corrective action plan for correcting the problems causing the exceptions or deficiencies and to implement the plan.

In the event of the audited entity's failure to develop such a corrective action plan or implement it, or if the report reveals exceptions or deficiencies that CERTISIGN and the audited entity's Superior Entity reasonably believe pose an immediate threat to the security or integrity of CERTISIGN TRUST NETWORK, then:
(a) CERTISIGN and/or the Superior Entity SHALL determine whether revocation and compromise reporting are necessary,
(b) CERTISIGN and the Superior Entity SHALL be entitled to suspend services to the audited entity, and
(c) If necessary, CERTISIGN and the Superior Entity MAY terminate such services subject to this CPS and the terms of the audited entity's contract with its Superior Entity.

8.6 Communications of Results

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in CP Section 7.1.6.1.

Following any Compliance Audit, the audited entity SHALL provide CERTISIGN and its Superior Entity (if the Superior Entity is not CERTISIGN) with the annual report and attestations based on its audit or self-audit within 14 days after the completion of the audit and no later than 45 days after the anniversary date of commencement of operations.

CERTISIGN TRUST NETWORK makes its annual Audit Report publicly available no later than three (3) months after the end of the audit period. In the event of a delay greater than three months, CERTISIGN TRUST NETWORK SHALL provide an explanatory letter signed by the Qualified Auditor.

8.7. Self-Audits

8.7.1. CABF Self-Audits Requirement

During the period in which the CA issues Certificates, CERTISIGN TRUST NETWORK SHALL monitor adherence to its CP, this CPS and these Requirements and strictly control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken. Except for Delegated Third Parties that undergo an annual audit that meets the criteria specified in Section 8.1, CERTISIGN TRUST NETWORK SHALL strictly control the service quality of Certificates issued or containing information verified by a Delegated Third Party by having a Validation Specialist employed by CERTISIGN TRUST NETWORK perform ongoing quarterly audits against a randomly selected sample of at least the greater of one certificate or three percent of the Certificates verified by the Delegated Third Party in the period beginning immediately after the last sample was taken. CERTISIGN TRUST NETWORK SHALL review each Delegated Third Party's practices and procedures to ensure that the Delegated Third Party is in compliance with these Requirements and the relevant CP and/or CPS.

CERTISIGN TRUST NETWORK SHALL internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the CA's CP and the Subordinate CA's CPS. On at least a quarterly basis, against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by the Subordinate CA, during the period commencing immediately after the previous audit sample was taken, the CA shall ensure all applicable CP are met.

8.7.2. Self-Audits Requirements for EV and EV Code Signing

During the period in which it issues EV and EV Code Signing Certificates, CERTISIGN MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least 3% of the EV and EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV and EV Code Signing Certificates where the Final Cross-Correlation and Due Diligence requirements of CP Appendix C, Item 13 is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least 6% of the EV and EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

CERTISIGN is entitled to charge end-user Subscribers for the issuance, management, and renewal of Certificates.

9.1.2 Certificate Access Fees

CERTISIGN does not charge a fee as a condition of making a Certificate available in a repository or otherwise making Certificates available to Relying Parties.

9.1.3 Revocation or Status Information Access Fees

CERTISIGN does not charge a fee as a condition of making the CRLs REQUIRED by the CP available in a repository or otherwise available to Relying Parties. CERTISIGN is, however, entitled to charge a fee for providing customized CRLs, OCSP services, or other value-added revocation and status information services. CERTISIGN does not permit access to revocation information, Certificate status information, or time stamping in their repositories by third parties that provide products or services that utilize such Certificate status information without CERTISIGN 's prior express written consent.

9.1.4 Fees for Other Services

CERTISIGN does not charge a fee for access to this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, SHALL be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

Within CERTISIGN 's Sub-domain, the following refund policy (reproduced at https://www.certisign.com.br/certisign/politicas/garantia-de-certificados-ssl) is in effect:

CERTISIGN adheres to, and stands behind, rigorous practices and policies in undertaking certification operations and in issuing certificates. Nevertheless, if for any reason a subscriber is not completely satisfied with the certificate issued to him, her, or it, the subscriber MAY request that CERTISIGN revoke the certificate within thirty (30) days of issuance and provide the subscriber with a refund. Following the initial thirty (30) day period, a subscriber MAY request that CERTISIGN revoke the certificate and provide a refund if CERTISIGN has breached a warranty or other material obligation under this CPS relating to the subscriber or the subscriber's certificate. After CERTISIGN revokes the subscriber's certificate, CERTISIGN will promptly credit the subscriber. To request a refund, please call customer service at https://www.certisign.com.br/atendimento-suporte/contato/fale-certisign . This refund policy is not an exclusive remedy and does not limit other remedies that MAY be available to subscribers.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

CERTISIGN, Affiliates and Enterprise Customers (when REQUIRED) SHALL maintain a commercially reasonable level of insurance coverage for errors and omissions, either through an errors and omissions insurance program with an insurance carrier or a self-insured retention. This insurance requirement does not apply to governmental entities.

9.2.2 Other Assets

CERTISIGN, Affiliates and Enterprise Customers SHALL have sufficient financial resources to maintain their operations and perform their duties, and they MUST be reasonably able to bear the risk of liability to Subscribers and Relying Parties.

9.2.3 Extended Warranty Coverage

Some CERTISIGN TRUST NETWORK participants offer extended warranty programs that provides SSL and code signing certificate subscribers with protection against loss or damage that is due to a defect in the participant's issuance of the certificate or other malfeasance caused by participant's negligence or breach of its contractual obligations, provided that the subscriber of the certificate has fulfilled its obligations under the applicable service agreement. CERTISIGN TRUST NETWORK participants offering extended warranty programs are REQUIRED to include program information in this CPS.

9.2.4 EV Certificates and EV Code Signing Certificates Insurance

CERTISIGN TRUST NETWORK maintains the following insurance related to their respective performance and obligations over EV Certificates:

(A) Commercial General Liability insurance (occurrence form) with policy limits of at least two million US dollars in coverage; and

(B) Professional Liability/Errors and Omissions insurance, with policy limits of at least five million US dollars in coverage, and including coverage for (i) claims for damages arising out of an act, error, or omission, unintentional breach of contract, or neglect in issuing or maintaining EV Certificates, and (ii) claims for damages arising out of infringement of the proprietary rights of any third party (excluding copyright, and trademark infringement), and invasion of privacy and advertising injury.

Such insurance MUST be with a company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies each of the members of which are so rated).

CERTISIGN TRUST NETWORK MAY self-insure for liabilities that arise from such party's performance and obligations under this Section 9.2.4 provided that it has at least five hundred million US dollars in liquid assets based on audited financial statements in the past twelve months, and a quick ratio (ratio of liquid assets to current liabilities) of not less than 1.0.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

The following records of Subscribers SHALL, subject to Section 9.3.2, be kept confidential and private ("Confidential/Private Information"):

- CA application records, whether approved or disapproved,
- Certificate Application records,
- Private keys held by enterprise Customers using Managed PKI SSL Certisign and information needed to recover such Private Keys,
- Transactional records (both full records and the audit trail of transactions),
- Audit trail records created or retained by CERTISIGN or a Customer,
- Audit reports created by CERTISIGN or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public),
- Contingency planning and disaster recovery plans, and
- Security measures controlling the operations of CERTISIGN hardware and software and the administration of Certificate services and designated enrollment services.

9.3.2 Information Not Within the Scope of Confidential Information

Certificates, Certificate revocation and other status information, CERTISIGN repositories and information contained within them are not considered Confidential/Private Information.

Information not expressly deemed Confidential/Private Information under Section 9.3.1 SHALL be considered neither confidential nor private. This section is subject to applicable privacy laws.

9.3.3 Responsibility to Protect Confidential Information

CERTISIGN TRUST NETWORK participants receiving private information SHALL secure it from compromise and disclosure to third parties.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

CERTISIGN and Affiliates SHALL implement a privacy policy in accordance with CERTISING internal requirements. Such privacy policies SHALL conform to applicable local privacy laws. CERTISIGN and Affiliates SHALL NOT disclose or sell the names of Certificate Applicants or other identifying information about them, subject to Section 9.3.2 and to the right of a terminating CA to transfer such information to a successor CA under Section 5.8.

CERTISIGN has implemented a Privacy Policy, which is located at https://www.certisign.com.br/certisign/politicas/privacidade, in compliance with this section.

9.4.2 Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, certificate directory and online CRLs is treated as private.

9.4.3 Information Not Deemed Private
Subject to local laws, all information made public in a certificate is deemed not private.

9.4.4 Responsibility to Protect Private Information
CERTISIGN TRUST NETWORK participants receiving private information SHALL secure it from compromise and disclosure to third parties and SHALL comply with all local privacy laws in their jurisdiction.

9.4.5 Notice and Consent to Use Private Information
Unless where otherwise stated in this CPS, the applicable Privacy Policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

This section is subject to applicable privacy laws.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process
CERTISIGN SHALL be entitled to disclose Confidential/Private Information if, in good faith, CERTISIGN believes that:

- disclosure is necessary in response to subpoenas and search warrants.
- disclosure is necessary in response to judicial, administrative, or other legal process during the discovery process in a civil or administrative action, such as subpoenas, interrogatories, requests for admission, and requests for production of documents.

This section is subject to applicable privacy laws.

9.4.7 Other Information Disclosure Circumstances
Privacy policies SHALL contain provisions relating to the disclosure of Confidential/Private Information to the person disclosing it to CERTISIGN or the Affiliate. This section is subject to applicable privacy laws.

9.5 Intellectual Property rights
The allocation of Intellectual Property Rights among CERTISIGN Sub-domain Participants other than Subscribers and Relying Parties is governed by the applicable agreements among such CERTISIGN Sub-domain Participants. The following subsections of Section 9.5 apply to the Intellectual Property Rights in relation to Subscribers and Relying Parties.

9.5.1 Property Rights in Certificates and Revocation Information
CAs retain all Intellectual Property Rights in and to the Certificates and revocation information that they issue. CERTISIGN and Customers grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate.

CERTISIGN and Customers SHALL grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL Usage Agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CPS
CERTISIGN TRUST NETWORK Participants acknowledge that CERTISIGN retains all Intellectual Property Rights in and to this CPS.

9.5.3 Property Rights in Names
A Certificate Applicant retains all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate Application and distinguished name within any Certificate issued to such Certificate Applicant.

9.5.4 Property Rights in Keys and Key Material

Key pairs corresponding to Certificates of CAs and end-user Subscribers are the property of the CAs and end-user Subscribers that are the respective Subjects of these Certificates, subject to the rights of enterprise Customers using Certigate, regardless of the physical medium within which they are stored and protected, and such persons retain all Intellectual Property Rights in and to these key pairs.

Without limiting the generality of the foregoing, Root CA public keys and the Root CA Certificates containing them, are the property of CERTISIGN. CERTISIGN licenses software and hardware manufacturers to reproduce such root Certificates to place copies in trustworthy hardware devices or software.

Finally, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from CERTISIGN.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

CERTISIGN TRUST NETWORK warrants that:

- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application or issuing the Certificate as a result of a failure to exercise reasonable care in managing the Certificate Application or creating the Certificate,
- Their Certificates meet all material requirements of this CPS and the applicable CP, and
- Revocation services and use of a repository conform to all material requirements of this CPS and the applicable CP in all material aspects.

9.6.1.1 CABF Warranties and Obligations

By issuing a Certificate, CERTISIGN TRUST NETWORK makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate.

CERTISIGN TRUST NETWORK represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, CERTISIGN TRUST NETWORK has complied with these Requirements and its CP and/or CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:
1. Right to Use Domain Name or IP Address: That, at the time of issuance, CERTISIGN TRUST NETWORK (i)implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii)followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in CERTISIGN TRUST NETWORK CP and/or CPS;
2. Authorization for Certificate: That, at the time of issuance, CERTISIGN TRUST NETWORK (i)implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii)followed the procedure when issuing the Certificate; and (iii)accurately described the procedure in CERTISIGN TRUST NETWORK CP and/or CPS;

3. Accuracy of Information: That, at the time of issuance, CERTISIGN TRUST NETWORK (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the *subject:organizationalUnitName* attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in CERTISIGN TRUST NETWORK CP and/or CPS;
4. No Misleading Information: That, at the time of issuance, CERTISIGN TRUST NETWORK (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's *subject:organizationalUnitName* attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in CERTISIGN TRUST NETWORK CP and/or CPS;
5. Identity of Applicant: That, if the Certificate contains Subject Identity Information, CERTISIGN TRUST NETWORK (i)implemented a procedure to verify the identity of the Applicant in accordance with CP Section 3.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in CERTISIGN TRUST NETWORK CP and/or CPS;
6. Subscriber Agreement: That, if CERTISIGN TRUST NETWORK and Subscriber are not Affiliated, the Subscriber and CERTISIGN TRUST NETWORK are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if CERTISIGN TRUST NETWORK and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
7. Status: That CERTISIGN TRUST NETWORK maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and
8. Revocation: That CERTISIGN TRUST NETWORK will revoke the Certificate for any of the reasons specified in these Requirements.

The Root CA SHALL be responsible for the performance and warranties of the Subordinate CA, for the Subordinate CA's compliance with these Requirements, and for all liabilities and indemnification obligations of the Subordinate CA under these Requirements, as if the Root CA were the Subordinate CA issuing the Certificates Subscriber Agreements MAY include additional representations and warranties.

9.6.1.2 Warranties for EV Certificate

When CERTISIGN TRUST NETWORK issues an EV Certificate, CERTISIGN TRUST NETWORK and its Root CA represent and warrant to the Certificate Beneficiaries listed in this Section, during the period when the EV Certificate is Valid, that CERTISIGN TRUST NETWORK has followed the requirements of CAB/FORUM Guidelines and its EV Policies in issuing and managing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate. The EV Certificate Warranties specifically include, but are not limited to, the following:
(A) Legal Existence: CERTISIGN TRUST NETWORK has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
(B) Identity: CERTISIGN TRUST NETWORK has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
(C) Right to Use Domain Name: CERTISIGN TRUST NETWORK has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) listed in the EV Certificate;
(D) Authorization for EV Certificate: CERTISIGN TRUST NETWORK has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate;
(E) Accuracy of Information: CERTISIGN TRUST NETWORK has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued;
(F) Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable

Subscriber Agreement with CERTISIGN TRUST NETWORK that satisfies the requirements of CAB/FORUM Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
(G) Status: CERTISIGN TRUST NETWORK will follow the requirements of CAB/FORUM Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and
(H) Revocation: CERTISIGN TRUST NETWORK will follow the requirements of CAB/FORUM Guidelines and revoke the EV Certificate for any of the revocation reasons specified in these Guidelines.

9.6.1.3 Warranties for EV Code Signing Certificate
When CERTISIGN TRUST NETWORK issues an EV Code Signing Certificate, CERTISIGN TRUST NETWORK and its Root CA represent and warrant to the Certificate Beneficiaries listed in this Section, during the period when the EV Code Signing Certificate is Valid, that CERTISIGN TRUST NETWORK has followed the requirements of CAB/FORUM Guidelines and its EV Code Signing Policies in issuing and managing the EV Code Signing Certificate and in verifying the accuracy of the information contained in the EV Code Signing Certificate. The EV Code Signing Certificate Warranties specifically include, but are not limited to, the following:
(A) Legal Existence: CERTISIGN TRUST NETWORK has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Code Signing Object was issued, the Subject of the EV Code Signing Object legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration;
(B) Identity: CERTISIGN TRUST NETWORK has confirmed that, as of the date the EV Code Signing Object was issued, the legal name of the Subject named in the EV Code Signing Object matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business;
(C) Right to Use Domain Name: CERTISIGN TRUST NETWORK has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) listed in the EV Code Signing Object;
(D) Authorization for EV Code Signing Certificate: CERTISIGN TRUST NETWORK has taken all steps reasonably necessary to verify that the Subject of the EV Code Signing Object authorized the issuance of the EV Code Signing Object;
(E) Accuracy of Information: CERTISIGN TRUST NETWORK has taken all steps reasonably necessary to verify that all of the other information in the EV Code Signing Object is accurate, as of the date of issuance;
(F) Subscriber Agreement: The Subject of the EV Code Signing Object has entered into a legally valid and enforceable Subscriber Agreement with the Issuer that satisfies the requirements of CAB/FORUM Guidelines or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use;
(G) Status: CERTISIGN TRUST NETWORK will follow the requirements of CAB/FORUM Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Code Signing Object as Valid or revoked; and
(H) Revocation: CERTISIGN TRUST NETWORK will follow the requirements of CAB/FORUM Guidelines and revoke the EV Code Signing Object for any of the revocation reasons specified in these Guidelines.

9.6.2 RA Representations and Warranties
CERTISIGN TRUST NETWORK RAs warrant that:
- There are no material misrepresentations of fact in the Certificate known to or originating from the entities approving the Certificate Application or issuing the Certificate,
- There are no errors in the information in the Certificate that were introduced by the entities approving the Certificate Application as a result of a failure to exercise reasonable care in managing the Certificate Application,
- Their Certificates meet all material requirements of this CPS and the applicable CPS and

- Revocation services (when applicable) and use of a repository conform to all material requirements of this CPS and the applicable CP in all material aspects.

Subscriber Agreements MAY include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

Subscribers warrant that:

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

Subscriber Agreements MAY include additional representations and warranties.

9.6.3.1 CABF Subscriber Agreement Requirements

CERTISIGN TRUST NETWORK requires, as part of the Subscriber Agreement or Terms of Use, that the Applicant make the commitments and warranties in this section for the benefit of CERTISIGN TRUST NETWORK and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, CERTISIGN TRUST NETWORK obtains, for the express benefit of CERTISIGN TRUST NETWORK and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with CERTISIGN TRUST NETWORK, or
2. The Applicant's acknowledgement of the Terms of Use.

CERTISIGN TRUST NETWORK implements a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. CERTISIGN TRUST NETWORK MAY use an electronic or "click-through" Agreement provided that CERTISIGN TRUST NETWORK has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that CERTISIGN TRUST NETWORK issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to CERTISIGN TRUST NETWORK, both in the certificate request and as otherwise requested by CERTISIGN TRUST NETWORK in connection with the issuance of the Certificate(s) to be supplied by CERTISIGN TRUST NETWORK;

2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the

Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);

3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;

4. Use of Certificate:
i. EV Certificates: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
ii. EV Code Signing Certificate: An obligation and warranty to not knowingly sign software that contains Suspect Code and use the EV Code Signing Certificate as follows:
a. only to sign code that complies with the requirements set forth in CABF Guidelines;
b. solely in compliance with all applicable laws;
c. solely for authorized company business; and
d. solely in accordance with the Subscriber Agreement;

5. Reporting and Revocation: An obligation and warranty to promptly request revocation of the Certificate, and cease using it and its associated Private Key, in the event that:
a. there is evidence that the certificate was used to sign suspect code – for EV Code Signing Certificate;
b. any information in the Certificate is, or becomes, incorrect or inaccurate; or
c. there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber's Private Key associated with the Public Key included in the Certificate;

6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise;

7. Responsiveness: An obligation to respond to CERTISIGN TRUST NETWORK instructions concerning Key Compromise or Certificate misuse within a specified time period.

8. Acknowledgment and Acceptance: An acknowledgment and acceptance that CERTISIGN TRUST NETWORK is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use or if CERTISIGN TRUST NETWORK discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

In case of EV Code Signing Certificate:
- If a Signing Authority becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, then it MUST immediately inform CERTISIGN TRUST NETWORK . If a Signing Authority's private key, or private key activation data, is compromised or believed to be compromised, the Signing Authority MUST contact CERTISIGN TRUST NETWORK immediately and request that the certificate be revoked.

- Signing Authorities MUST obtain a Subscriber or Terms of Use Agreement with its customer that contains the following obligations and warranties:
1. To use the EV Signature solely in compliance with the requirements set forth herein and the applicable EV Guidelines;
2. To use the EV Signature solely in compliance with all applicable laws;
3. To use the EV Signature solely for authorized company business;
4. To use the EV Signature solely in accordance with the Subscriber or Terms of Use Agreement;
5. To not knowingly submit software for signature that contains Suspect Code;
6. To inform the Signing Authority if it is discovered (by whatever means) that code submitted to the

Signing Authority for signature contains malware or a serious vulnerability.

9.6.5 Representations and Warranties of Other Participants
No stipulation.

9.7 Disclaimers of Warranties
To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL disclaim CERTISIGN 's possible warranties, including any warranty of merchantability or fitness for a particular purpose, outside the context of CERTISIGN TRUST NETWORK CPS.

9.8 Limitations of Liability
To the extent CERTISIGN has issued and managed the Certificate(s) at issue in compliance with its Certificate Policy and its Certification Practice Statement, CERTISIGN SHALL have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). Limitations of liability SHALL include an exclusion of indirect, special, incidental, and consequential damages. They SHALL also observOne Hundred U.S. Dollars ($ 100.00 US) liability caps limiting CERTISIGN 's and the Affiliate's damages.

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.

For delegated tasks, CERTISIGN TRUST NETWORK and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but CERTISIGN TRUST NETWORK remains fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.
If CERTISIGN TRUST NETWORK has issued and managed the Certificate in compliance with these Requirements and its CP and/or CPS, CERTISIGN TRUST NETWORK disclaims liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in CERTISIGN TRUST NETWORK CP and/or CPS.
If CERTISIGN TRUST NETWORK has not issued or managed the Certificate in compliance with these Requirements and its CP and/or CPS, CERTISIGN TRUST NETWORK seeks to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that it desires. If CERTISIGN TRUST NETWORK chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its CP and/or CPS, then CERTISIGN TRUST NETWORK will include the limitations on liability in CERTISIGN TRUST NETWORK CP and/or CPS.

9.8.1 CABF Limitations of Liability Requirements
For delegated tasks, CERTISIGN TRUST NETWORK and any Delegated Third Party MAY allocate liability between themselves contractually as they determine, but the CA SHALL remain fully responsible for the performance of all parties in accordance with these Requirements, as if the tasks had not been delegated.

If CERTISIGN TRUST NETWORK has issued and managed the Certificate in compliance with CABF Requirements and its CP and/or CPS, CERTISIGN TRUST NETWORK MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in CERTISIGN TRUST NETWORK CP and/or CPS. If CERTISIGN TRUST NETWORK has not issued or managed the

Certificate in compliance with CABF Requirements and its CP and/or CPS, CERTISIGN TRUST NETWORK MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that CERTISIGN TRUST NETWORK desires. If CERTISIGN TRUST NETWORK chooses to limit its liability for Certificates that are not issued or managed in compliance with CABF Requirements or its CP and/or CPS, then the CA SHALL include the limitations on liability in CERTISIGN TRUST NETWORK CP and/or CPS.

9.8.2 Limitations of Liability for EV

CERTISIGN MAY limit its liability as described in this Section 9.8 except that CERTISIGN MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV Certificate.
CA's indemnification obligations and a Root CA's obligations with respect to subordinate CAs are set forth in Section 9.9 below.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

To the extent permitted by applicable law, Subscribers are REQUIRED to indemnify CERTISIGN for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's private key, to use a Trustworthy System, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the Intellectual Property Rights of a third party.

The applicable Subscriber Agreement MAY include additional indemnity obligations.

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, CERTISIGN TRUST NETWORK understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of CERTISIGN TRUST NETWORK under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, CERTISIGN TRUST NETWORK defends, indemnifies, and holds harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by CERTISIGN TRUST NETWORK, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by CERTISIGN TRUST NETWORK 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 CERTISIGN TRUST NETWORK online, and the application software either failed to check such status or ignored an indication of revoked status).

9.9.2 Indemnification by Relying Parties

To the extent permitted by applicable law, Relying Party Agreements SHALL require Relying Parties to indemnify CERTISIGN for:

- The Relying Party's failure to perform the obligations of a Relying Party,
- The Relying Party's reliance on a Certificate that is not reasonable under the circumstances, or
- The Relying Party's failure to check the status of such Certificate to determine if the Certificate is expired or revoked.

The applicable Relying Party Agreement MAY include additional indemnity obligations.

9.9.3 Indemnification of Application Software Suppliers

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the CERTISIGN Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others.

Thus the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA 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 the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and Termination

9.10.1 Term

The CPS becomes effective upon publication in the CERTISIGN Repository. Amendments to this CPS become effective upon publication in the CERTISIGN Repository.

9.10.2 Termination

This CPS as amended from time to time SHALL remain in force until it is replaced by a new version.

9.10.3 Effect of Termination and Survival

Upon termination of this CPS, CERTISIGN Sub-domain participants are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

9.11 Individual Notices and Communications with Participants

Unless otherwise specified by agreement between the parties, CERTISIGN Sub-domain participants SHALL use commercially reasonable methods to communicate with each other, taking into account the criticality and subject matter of the communication.

9.12 Amendments

9.12.1 Procedure for Amendment

Amendments to this CPS MAY be made by the CERTISIGN Trust Network Policy Management Authority. Amendments SHALL either be in the form of a document containing an amended form of the CP or an update. Updates supersede any designated or conflicting provisions of the referenced version of the CP. The PMD SHALL determine whether changes to the CP require a change in the CP object identifiers of the Certificate policies corresponding to each type of Certificate.

9.12.2 Notification Mechanism and Period

CERTISIGN and the PMD reserve the right to amend the CP without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The PMD's decision to designate amendments as material or non-material SHALL be within the PMD's sole discretion.

The PMD SHALL send Affiliates notice of material amendments to the CP proposed by the PMD. The notice SHALL state the text of the proposed amendments and the comment period. Affiliates SHALL publish or provide a link to the proposed amendments on their own web-based repositories within a reasonable time after receiving notice of such amendments.

The PMD solicits proposed amendments to the CP from other CERTISIGN TRUST NETWORK Participants. If the PMD considers such an amendment desirable and proposes to implement the amendment, the PMD SHALL provide notice of such amendment in accordance with this section.

Notwithstanding anything in the CP to the contrary, if the PMD believes that material amendments to the CP are necessary immediately to stop or prevent a breach of the security of CERTISIGN TRUST NETWORK or any portion of it, CERTISIGN and the PMD SHALL be entitled to make such amendments by publication in the CERTISIGN Repository. Such amendments will be effective immediately upon publication. Within a reasonable time after publication, CERTISIGN SHALL provide notice to Affiliates of such amendments.

9.12.2.1 Comment Period

Except as otherwise stated, the comment period for any material amendments to the CP SHALL be 15 days, starting on the date on which the amendments are posted on the CERTISIGN Repository. Any CERTISIGN TRUST NETWORK Participant SHALL be entitled to file comments with the PMD up until the end of the comment period.

9.12.2.2 Mechanism to Handle Comments

The PMD SHALL consider any comments on the proposed amendments. The PMD SHALL either
(a) allow the proposed amendments to become effective without amendment,
(b) amend the proposed amendments and republish them as a new amendment when REQUIRED, or
(c) withdraw the proposed amendments.

The PMD is entitled to withdraw proposed amendments by notifying Affiliates and providing notice in the Practices Updates and Notices section of the CERTISIGN Repository. Unless proposed amendments are amended or withdrawn, they SHALL become effective upon the expiration of the comment period.

9.12.3 Circumstances under Which OID Must be Changed

If the PMD 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 type of Certificate. Otherwise, amendments SHALL NOT require a change in Certificate policy object identifier.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among CERTISIGN, Affiliates, and Customers

Disputes among one or more of any of CERTISIGN, Affiliates, and/or Customers SHALL be resolved pursuant to provisions in the applicable agreements among the parties.

9.13.2 Disputes with End-User Subscribers or Relying Parties

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL contain a dispute resolution clause. Disputes involving CERTISIGN require an initial negotiation period of sixty (60) days followed by litigation in the city court of São Paulo, Brasil.

9.14 Governing Law

Subject to any limits appearing in applicable law, the laws of the Brasil SHALL govern the enforceability, construction, interpretation, and validity of this CPS, irrespective of contract or other choice of law provisions. This choice of law is made to ensure uniform procedures and interpretation for all CERTISIGN TRUST NETWORK Participants, no matter where they are located.

This governing law provision applies only to this CPS. Agreements incorporating the CPS by reference MAY have their own governing law provisions, provided that this Section governs the enforceability, construction, interpretation, and validity of the terms of the CPS separate and apart from the remaining provisions of any such agreements, subject to any limitations appearing in applicable law.

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

If a court or government body with jurisdiction over the activities covered by this CPS and its CP determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise its Guidelines accordingly.

9.15 Compliance with Applicable Law

This CPS is subject to applicable national, state, local and foreign laws, rules, regulations, ordinances, decrees, and orders including, but not limited to, restrictions on exporting or importing software, hardware, or technical information.

9.15.1 Compliance with CABFORUM

Not applicable.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which CERTISIGN TRUST NETWORK operates or issues certificates, CERTISIGN TRUST NETWORK MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, CERTISIGN TRUST NETWORK SHALL immediately (and prior to issuing a certificate under the modified requirement) include in this Section a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by CERTISIGN TRUST NETWORK.

9.16.3.1 CABF Severability Requirements

CERTISIGN TRUST NETWORK MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to this CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum MAY designate), so that the CA/Browser Forum MAY consider possible revisions to these Requirements accordingly.

Any modification to CERTISIGN TRUST NETWORK practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

9.16.4 Enforcement (Attorney's Fees and Waiver of Rights)

Not applicable

9.16.5 Force Majeure

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements SHALL include a force majeure clause protecting CERTISIGN and the applicable Affiliate.

9.17 Other Provisions

Not applicable.

Appendix A: Table of Acronyms and Definitions

Term	Definition
AC Digital Notarization Service	A service offered to Managed PKI SSL Certisign Customers that provides a digitally signed assertion (a Digital Receipt) that a particular document or set of data existed at a particular point in time
AC Participant	An individual or organization that is one or more of the following within AC: CERTISIGN, an Affiliate, a Customer, a Reseller, a Subscriber, or a Relying Party
AC PKI	consists of systems that collaborate to provide and implement AC
AC Repository	CERTISIGN's database of Certificates and other relevant CERTISIGN SSL CERTIFICATION AUTHORITY information accessible on-line
AC Standards	The business, legal, and technical requirements for issuing, managing, revoking, renewing, and using Certificates within AC
Accounting Practitioner	A certified public accountant, chartered accountant, or a person with an equivalent license within the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility; provided that an accounting standards body in the jurisdiction maintains full (not "suspended" or "associate") membership status with the International Federation of Accountants.
ACS	Authenticated Content Signing
Administrator	A Trusted Person within the organization of a CA or AR that performs validation and other CA or RA functions
Administrator Certificate	A Certificate issued to an Administrator that MAY only be used to perform CA or RA functions
Affiliate	A trusted third party(corporation, partnership, joint venture or other entity controlling, controlled by, or under common control with another entity, or an agency, department, political subdivision, or any entity operating under the direct control of a Government Entity) that has entered into an agreement with CERTISIGN to be a CA distribution and services channel within a specific territory
Affiliated Individual	A natural person that is (i) as an officer, director, employee, partner, contractor, intern, or other person within the Affiliate; (ii) as a member of a CERTISIGN registered community of interest, or (iii) as a person maintaining a relationship with the entity where the entity has business or other records providing appropriate assurances of the identity of such person
AICPA	American Institute of Certified Public Accountants
ANSI	The American National Standards Institute
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 or human sponsor 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 AC or is the CA.
Application Software Supplier	A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root 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
Audit Period	In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1
Audit Report	A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these

	Requirements
Authorization Domain Name	The Domain Name used to obtain authorization for certificate issuance for a given FQDN. AC MAY use the FQDN returned from a DNS CNAME lookup as the FQDN for the purposes of domain validation. If the FQDN contains a wildcard character, then AC MUST remove all wildcard labels from the left most portion of requested FQDN. AC 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 (http), 25 (smtp), 22 (ssh).
Automated Administration	A procedure whereby Certificate Applications are approved automatically if enrollment information matches information contained in a database
Automated Administration Software Module	Software provided by CERTISIGN that performs Automated Administration
Base Domain Name	The portion of an applied-for FQDN that is the first domain name node left of a registrycontrolled 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.
BIPM	International Bureau of Weights and Measures
BIS	(US Government) Bureau of Industry and Security
Business Entity	Any entity that is not a Private Organization, Government Entity, or Non-Commercial Entity as defined herein. Examples include, but are not limited to, general partnerships, unincorporated associations, sole proprietorships, etc.
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CEO	Chief Executive Officer
Certificate	An electronic document that uses a digital signature to bind a public key and an identity. At least, it states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, identifies the Certificate's Operational Period, contains a Certificate serial number, and is digitally signed by the CA.
Certificate Applicant	An individual or organization that requests the issuance of a Certificate by a CA
Certificate Application	A request from a Certificate Applicant (or authorized agent of the Certificate Applicant) to a CA for the issuance of a Certificate
Certificate Approver	A natural person who is either the Applicant, employed by the Applicant, or an authorized agente 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.
Certificate Chain	An ordered list of Certificates containing an end-user Subscriber Certificate and CA Certificates, which terminates in a root Certificate
Certificate Data	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
Certificate Management Control Objectives	Criteria that an entity MUST meet in order to satisfy a Compliance Audit
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which AC verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates
Certificate Policy (CP)	A set of rules that indicates the applicability of a named Certificate to a particular community and/or PKI implementation with common security requirements.
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 an EV Certificate Request on behalf of the Applicant.
Certificate Revocation List (CRL)	A periodically (or exigently) issued list, digitally signed by a CA, of identified Certificates that have been revoked prior to their expiration dates in accordance with CP Section 3.4. The list generally indicates the CRL issuer's name, the date of issue, the date of the next scheduled CRL issue, the revoked Certificates' serial numbers, and the specific times and reasons for revocation
Certificate Signing Request (CSR)	A message conveying a request to have a Certificate issued
Certification Authority (CA)	An organization that is responsible for the creation, issuance, revocation and management of Certificates. The term applies equally to both Roots CAs and Subordinate CAs.
Certification Authority Authorization (CAA)	From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource Recor ds allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate misissue"
Certification Practice Statement (CPS)	One of several documents forming the governance framework in which Certificates are created, issued, managed, and used. A statement of the practices that CERTISIGN or an Affiliate employs in approving or rejecting Certificate Applications and issuing, managing, and revoking Certificates.
CERTISIGN	Means, with respect to each pertinent portion of this CPS, CERTISIGN Certificadora Digital S.A. and/or any wholly owned CERTISIGN subsidiary responsible for the specific operations at issue
CERTISIGN SSL CERTIFICATION AUTHORITY	The Certificate-based Public Key Infrastructure governed by AC Certificate Policies, which enables the worldwide deployment and use of Certificates by CERTISIGN and its Affiliates, and their respective Customers, Subscribers, and Relying Parties
CFO	Chief Financial Officer
Challenge Phrase	A secret phrase chosen by a Certificate Applicant during enrollment for a Certificate. When issued a Certificate, the Certificate Applicant becomes a Subscriber and a CA or RA can use the Challenge Phrase to authenticate the Subscriber when the Subscriber seeks to revoke or renew the Subscriber's Certificate
CICA	Canadian Institute of Chartered Accountants
CIO	Chief Information Officer
CISO	Chief Information Security Officer
Compliance Audit	A periodic audit that a AC or AR undergoes to determine its conformance with AC Standards that apply to it
Compromise	A violation (or suspected violation) of a security policy, in which an unauthorized disclosure of, or loss of control over, sensitive information MAY have occurred. With respect to private keys, a Compromise is a loss, theft, disclosure, modification, unauthorized use, or other compromise of the security of such private key
Confidential/Private Information	Information required to be kept confidential and private pursuant to CP Section 2.8.1
Confirmation Request	An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.
Confirming Person	A position within an Applicant's organization that confirms the particular fact at issue
Contract Signer	A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
Control	"Control" (and its correlative meanings, "controlled by" and "under common control with") means possession, directly or indirectly, of the power to: (1) direct the management, personnel, finances, or plans of such entity; (2) control the election of a majority of the directors ; or (3) vote that portion of voting shares required for "control" under the law of the entity's Jurisdiction of Incorporation or Registration but in no case less than 10%.
COO	Chief Operating Officer
Country	Either a member of the United Nations OR a geographic region recognized as a Sovereign

	State by at least two UN member nations.
CP	Certificate Policy
CPA	Chartered Professional Accountant
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CRL Usage Agreement	An agreement setting forth the terms and conditions under which a CRL or the information in it can be used
Cross Certificate	A certificate that is used to establish a trust relationship between two Root CAs
CSO	Chief Security Officer
CSPRNG	A random number generator intended for use in cryptographic system.
Customer	An organization that is either a Managed PKI SSL Certisign Customer or Gateway Customer
DBA	Doing Business As
Delegated Third Party	A natural person or Legal Entity that is not the CA, and whose activities are not within the scope of the appropriate CA audits, but is authorized by the CA to assist in the Certificate Management Process by performing or fulfilling one or more of the CA requirements found herein.
Demand Deposit Account	A deposit account held at a bank or other financial institution, the funds deposited in which are payable on demand. The primary purpose of demand accounts is to facilitate cashless payments by means of check, bank draft, direct debit, electronic funds transfer, etc. Usage varies among countries, but a demand deposit account is commonly known as a share draft account, a current account, or a checking account.
DNS	Domain Name System
DNS CAA Email Contact	The email address defined in section J.1.1.
DNS TXT Record Email Contact	The email address defined in section J.2.1.
Domain Authorization	Correspondence or other documentation provided by a Domain Name Registrant attesting to the authority of an Applicant to request a Certificate for a specific Domain Namespace
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 or as obtained through direct contact with the Domain Name Registrar
Domain Name	The label assigned to a 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)
Domain Namespace	The set of all possible Domain Names that are subordinate to a single node in the Domain Name System.
Enterprise EV Certificate	An EV Certificate that an Enterprise RA authorizes the CA to issue at third and higher domain levels.
Enterprise EV RA	An RA that is authorized by the CA to authorize the CA to issue EV Certificates at third and higher domain levels
Enterprise RA	An employee or agent of an organization unaffiliated with AC who authorizes issuance of Certificates to that organization
Entry Date	The "Not After" date in a Certificate that defines the end of a Certificate's validity period
EV	Extended Validation

EV Authority	A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the EV Certificate Request, to take the Request actions described in these Guidelines
EV Certificate	A digital certificate that contains information specified in the EV Guidelines and that has been validated in accordance with the Guidelines
EV Certificate Beneficiaries	Persons to whom the CA and its Root CA make specified EV Certificate Warranties
EV Certificate Reissuance	The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a 'valid to' date that matches that of the current EV Certificate
EV Certificate Renewal	The process whereby an Applicant who has a valid unexpired and non-revoked EV Certificate makes an application, to the CA that issued the original certificate, for a newly issued EV Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing EV Certificate but with a new 'valid to' date beyond the expiry of the current EV Certificate
EV Certificate Request	A request from an Applicant to the CA requesting that the CA issue an EV Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Applicant Representative.
EV Certificate Warranties	In conjunction with the CA issuing an EV Certificate, the CA and its Root CA, during the period when the EV Certificate is Valid, promise that the CA has followed the requirements of these Guidelines and the CA's EV Policies in issuing the EV Certificate and in verifying the accuracy of the information contained in the EV Certificate
EV Code Signing Certificate	A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with these Guidelines
EV Code Signing Certificate Issuer	A CA providing an EV Code Signing Certificate to a Subscriber or a Signing Authority that provides an EV signature for a Subscriber.
EV Code Signing Object	An EV Code Signing Certificate issued by a CA or an EV Signature provided by a Signing Authority.
EV OID	An identifying number, in the form of an "object identifier," that is included in the *certificatePolicies* field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) is either the CA/Browser Forum EV policy identifier or a policy identifier that, by pre-agreement with one or more Application Software Supplier, marks the certificate as being an EV Certificate.
EV Policies	Auditable EV Certificate practices, policies and procedures, such as a certification practice statement and certificate policy, that are developed, implemented, and enforced by the CA and its Root CA
EV Processes	The keys, software, processes, and procedures by which the CA verifies Certificate Data under CA/Browser Forum EV Guidelines, issues EV Certificates, maintains a Repository, and revokes EV Certificates
EV Signature	An encrypted electronic data file which is attached to or logically associated with other electronic data and which (i) identifies and is uniquely linked to the signatory of the electronic data, (ii) is created using means that the signatory can maintain under its sole control, and (iii) is linked in a way so as to make any subsequent changes that have been made to the electronic data detectable.
EV Subscriber	The Subject of the EV Code Signing Certificate. A Subscriber is the entity responsible for distributing the software but does not necessarily hold the copyright to the software
Exigent Audit/Investigation	An audit or investigation by CERTISIGN where CERTISIGN has reason to believe that an entity's failure to meet AC Standards, an incident or Compromise relating to the entity, or an actual or potential threat to the security of AC posed by the entity has occurred
Extended Validation	Validation Procedures defined by the Guidelines for Extended Validation Certificates published by a forum consisting of major certification authorities and browser vendors
Extended Validation Certificate	EV Certificate
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully-Qualified Domain Name

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 context of a Private Organization, the government agency is in the Jurisdiction of Incorporation under whose authority the legal existence of Private Organizations is established (e.g., the government agency that issued the Certificate of Incorporation) . In the context of Business Entities, the government agency in the jurisdiction of operation that registers business entities. . In the case of a Government Entity, is a government-operated legal entity, agency, department, ministry, branch, or similar element of the government of a country, or political subdivision within such country (such as a state, province, city, country, etc.)
gTLD	Generic TopLevel Domain
High Risk Certificate Request	A Request that AC flags for additional scrutiny by reference to internal criteria and databases maintained by the CA, which MAY include names at higher risk for phishing or other fraudulent usage, names contained in previously rejected certificate requests or revoked Certificates, nameslisted on the Miller Smiles phishing list or the Google Safe Browsing list, or names that AC identifies using its own risk-mitigation criteria.
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IFAC	International Federation of Accountants
IM	Instant Messaging
Incorporating Agency	Government Agency
Independent Confirmation From Applicant	Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.
Individual	A natural person
Intellectual Property Rights	Rights under one or more of the following: any copyright, patent, trade secret, trademark, and any other intellectual property rights
Intermediate Certification Authority	A Certification Authority whose Certificate is located within a Certificate Chain between the Certificate of the root CA and the Certificate of the Certification Authority that issued the end-user Subscriber's Certificate
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.
Internal Server Name	A Server Name (which MAY or MAY NOT include an Unregistered Domain Name) that is not resolvable using the public DNS
International Organization	An organization founded by a constituent document, e.g., a charter, treaty, convention or similar document, signed by, or on behalf of, a minimum of two Sovereign State governments
IRS	Internal Revenue Service
ISO	International Organization for Standardization
ISP	Internet Service Provider
Issuing CA	In relation to a particular Certificate, AC that issued the Certificate. This could be either a Root CA or a Subordinate CA
Jurisdiction of Incorporation	In the context 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 context of a Government Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.
Jurisdiction of Registration	In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person or an unauthorized person has had access to it.
Key Generation Ceremony	A procedure whereby a CA's or RA's key pair is generated, its private key is transferred into a cryptographic module, its private key is backed up, and/or its public key is certified.

Key Generation Script	A documented plan of procedures for the generation of a CA Key Pair
Key Manager Administrator	An Administrator that performs key generation and recovery functions for a Managed PKI SSL Certisign Customer using Certigate
Key Pair	The Private Key and its associated Public Key
Key Recovery Block (KRB)	A data structure containing a Subscriber's private key that is encrypted using an encryption key. KRBs are generated using Certigate software
Key Recovery Service	A CERTISIGN service that provides encryption keys needed to recover a Key Recovery Block as part of a Managed PKI SSL Certisign Customer's use of Certigate to recover a Subscriber's private key
KRB	Key Recovery Block
Latin Notary	A person with legal training whose commission under applicable law not only includes authority to authenticate the execution of a signature on a document but also responsibility for the correctness and content of the document. A Latin Notary is sometimes referred to as a Civil Law Notary.
Legal Entity	An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system
Legal Existence	A Private Organization, Government Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.
Legal Practitioner	A person who is either a lawyer or a Latin Notary as described in these Guidelines and competent to render an opinion on factual claims of the Applicant.
LSVA	Logical security vulnerability assessment
Managed PKI SSL Certisign	CERTISIGN's fully integrated Managed PKI SSL Certisign service that allows enterprise Customers of CERTISIGN and its Affiliates to distribute Certificates to individuals, such as employees, partners, suppliers, and customers, as well as devices, such as servers, routers, and firewalls. Managed PKI SSL Certisign permits enterprises to secure messaging, intranet28, extranet, virtual private network, and e-commerce applications
Managed PKI SSL Certisign Administrator	An Administrator that performs validation or other RA functions for a Managed PKI SSL Certisign Customer
Manual Authentication	A procedure whereby Certificate Applications are reviewed and approved manually one-by-one by an Administrator using a web-based interface
NIST	(US Government) National Institute of Standards and Technology
Non-repudiation	An attribute of a communication that provides protection against a party to a communication falsely denying its origin, denying that it was submitted, or denying its delivery. Denial of origin includes the denial that a communication originated from the same source as a sequence of one or more prior messages, even if the identity associated with the sender is unknown. Note: only an adjudication by a court, arbitration panel, or other tribunal can ultimately prevent repudiation. For example, a digital signature verified with reference to a AC Certificate MAY provide proof in support of a determination of Non-repudiation by a tribunal, but does not by itself constitute Non-repudiation
Non-verified Subscriber Information	Information submitted by a Certificate Applicant to a CA or RA, and included within a Certificate, that has not been confirmed by AC or RA and for which the applicable CA and RA provide no assurances other than that the information was submitted by the Certificate Applicant
Notary	A person whose commission under applicable law includes authority to authenticate the execution of a signature on a document.
Object Identifier	A unique alphanumeric or numeric identifier registered under the International Organization for Standardization's applicable standard for a specific object or object class
OCSP	Online Certificate Status Protocol
OCSP Responder	An online server operated under the authority of AC and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol
Offline CA	Issuing Root CAs and other designated intermediate CAs that are maintained offline for security reasons in order to protect them from possible attacks by intruders by way of the network. These CAs do not directly sign end user Subscriber Certificates
OID	Object Identifier
Online CA	CAs that sign end user Subscriber Certificates are maintained online so as to provide

	continuous signing services
Online Certificate Status Protocol	An online Certificate-checking protocol for providing Relying Parties with real-time Certificate status information
Operational Period	The period starting with the date and time a Certificate is issued (or on a later date and time certain if stated in the Certificate) and ending with the date and time on which the Certificate expires or is earlier revoked
Parent Company	A company that Controls a Subsidiary Company.
PIN	Personal identification number
PKCS	Public-Key Cryptography Standard
PKCS #10	Public-Key Cryptography Standard #10, developed by RSA Security Inc., which defines a structure for a Certificate Signing Request
PKCS #12	Public-Key Cryptography Standard #12, developed by RSA Security Inc., which defines a secure means for the transfer of private keys
PKI	Public Key Infrastructure
Place of Business	The location of any facility (such as a factory, retail store, warehouse, etc) where the Applicant's business is conducted
PMD	Policy Management Department
Policy Management Authority (PMD)	The organization within CERTISIGN responsible for promulgating this policy throughout AC
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 EV 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 or equivalent 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	The architecture, organization, techniques, practices, procedures, hardware, software, people, rules, policies, and obligations that collectively support the implementation and operation of a Certificate-based public key cryptographic system.
Publicly-Trusted Certificate	A Certificate that is trusted by virtue of the fact that its corresponding Root Certificate is distributed as a trust anchor in widely-available application software
QGIS	Qualified Government Information Source
QIIS	Qualified Independent Information Source
QTIS	Qualified Government Tax Information Source
Qualified Auditor	A natural person or Legal Entity that meets the requirements of Section 8.2 Identity/Qualifications of Assessor
Qualified Government Information Source	A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 11.11.6.
Qualified Government Tax Information Source	A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals
Qualified Independent Information Source	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.
RA	Registration Authority
Random Value	A value specified by a CA to the Applicant that exhibits at least 112 bits of entropy.
Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar.

Registered Domain Name	A Domain Name that has been registered with a Domain Name Registrar. Reliable Data Source: An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
Registered Office	The official address of a company, as recorded with the Incorporating Agency, to which oficial 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 or Office of Thrift Supervision.
Registration Authority	A Legal Entity that is responsible for identification and authentication of subjects of Certificates, but is not a CA, and hence does not sign or issue Certificates. An RA MAY assist in the certificate application process or revocation process or both. When "RA" is used as an adjective to describe a role or function, it does not necessarily imply a separate body, but can be part of the CA.
Registration Number	The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation
Regulated Financial Institution	A financial institution that is regulated, supervised, and examined by governmental, national, state or provincial, or local authorities.
Reliable Data Source	An identification document or source of data used to verify Subject Identity Information that is generally recognized among commercial enterprises and governments as reliable, and which was created by a third party for a purpose other than the Applicant obtaining a Certificate.
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 natural person or Legal Entity that relies on a Valid Certificate. An Application Software Supplier is not considered a Relying Party when software distributed by such Supplier merely displays information relating to a Certificate.
Relying Party Agreement	An agreement used by a CA setting forth the terms and conditions under which an individual or organization acts as a Relying Party.
Repository	An online database containing publicly-disclosed PKI governance documents (such as Certificate Policies and Certification Practice Statements) and Certificate status information, either in the form of a CRL or an OCSP response
Request Token	A value derived in a method specified by AC which binds this demonstration of control to the certificate request. The Request Token SHALL incorporate the key used in the certificate request. A Request Token MAY include a timestamp to indicate when it was created. A Request Token MAY include other information to ensure its uniqueness. A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation. A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future. A Request Token that does not include a timestamp is valid for a single use and AC SHALL NOT re-use it for a subsequent validation. The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.
Required Website Content	Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.
Reserved IP Address	An IPv4 or IPv6 address that the IANA has marked as reserved: http://www.iana.org/assignments/ipv4-address-space/ipv4-address-space.xml http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml
Retail Certificate	A Certificate issued by CERTISIGN or an Affiliate, acting as CA, to individuals or

	organizations applying one by one to CERTISIGN or an Affiliate on its web site.
RFC	Request for comment
Root CA	Root Certification Authority
Root Certificate	The self-signed Certificate issued by the Root CA to identify itself and to facilitate verification of Certificates issued to its Subordinate CAs
Root Certification Authority	A CA that acts as a root CA and issues Certificates to CAs subordinate to it
Root Key Generation Script	Key Generation Script of a Root CA Key Pair
RSA	A public key cryptographic system invented by Rivest, Shamir, and Adelman
S/MIME	Secure MIME (multipurpose Internet mail extensions)
SAR	Security Audit Requirements
SEC	(US Government) Securities and Exchange Commission
Secret Share	A portion of a CA private key or a portion of the activation data needed to operate a CA private key under a Secret Sharing arrangement
Secret Sharing	The practice of splitting a CA private key or the activation data to operate a CA private key in order to enforce multi-person control over CA private key operations under CP Section 6.2.2
Secure Sockets Layer	The industry-standard method for protecting Web communications developed by Netscape Communications Corporation. The SSL security protocol provides data encryption, server authentication, message integrity, and OPTIONAL client authentication for a Transmission Control Protocol/Internet Protocol connection
Security and Practices Review	A review of an Affiliate performed by CERTISIGN before an Affiliate is permitted to become operational
Signing Authority	One or more Certificate Approvers designated to act on behalf of the Applicant.
SOC	Service Organization Control standard
Sovereign State	A state or country that administers its own government, and is not dependent upon, or subject to, another power.
SSL	Secure Sockets Layer
SSL Admin	A web-based interface that permits Managed PKI SSL Certisign Administrators to perform Manual Authentication of Certificate Applications
Sub-domain	The portion of CERTISIGN AC PARCERIA under control of an entity and all entities subordinate to it within CERTISIGN AC PARCERIA hierarchy
Subject	The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject and holder of a private key corresponding to a public key. The Subject is either the Subscriber or a device under the control and operation of the Subscriber. The term “Subject” can, in the case of an organizational Certificate, refer to the equipment or device that holds a private key. A Subject is assigned an unambiguous name, which is bound to the public key contained in the Subject’s Certificate
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 Certificate is signed by the Root CA, or another Subordinate CA
Subscriber	In the case of an individual Certificate, a person who is the Subject of, and has been issued, a Certificate. In the case of an organizational Certificate, an organization that owns the equipment or device that is the Subject of, and that has been issued, a Certificate. A Subscriber is capable of using, and is authorized to use, the private key that corresponds to the public key listed in the Certificate
Subscriber Agreement	Subscriber Agreement: An agreement between CERTISIGN AC PARCERIA or RA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.
Subsidiary Company	A company that is controlled by a Parent Company.
Superior Entity	An entity above a certain entity within a CERTISIGN AC PARCERIA hierarchy
Superior Government Entity	Based on the structure of government in a political subdivision, the Government Entity or Entities that have the ability to manage, direct and control the activities of the Applicant.
Supplemental Risk	A review of an entity by CERTISIGN following incomplete or exceptional findings in a

Management Review	Compliance Audit of the entity or as part of the overall risk management process in the ordinary course of business
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.
Technically Constrained Subordinate CA Certificate	A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate MAY issue Subscriber or additional Subordinate CA Certificates.
Terms of Use	Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.
Test Certificate	A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID(2.23.140.2.1), or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.
Timestamp Authority	An organization that timestamps data, thereby asserting that the data existed at the specified time
TLD	Top-Level Domain
TLS	Transport Layer Security
Translator	An individual or Business Entity that possesses the requisite knowledge and expertise to accurately translate the words of a document written in one language to the native language of the CA.
Trusted Person	An employee, contractor, or consultant of an entity within CERTISIGN AC PARCERIA responsible for managing infrastructural trustworthiness of the entity, its products, its services, its facilities, and/or its practices as further defined in CP Section 5.2.1
Trusted Position	The positions within a CERTISIGN AC PARCERIA entity that MUST be held by a Trusted Person.
Trustworthy System	Computer hardware, software, and procedures that are reasonably secure from intrusion and misuse; provide a reasonable level of availability, reliability, and correct operation; are reasonably suited to performing their intended functions; and enforce the applicable security policy. A trustworthy system is not necessarily a “trusted system” as recognized in classified government nomenclature
TTL	Time To Live
Unregistered Domain Name	A Domain Name that is not a Registered Domain Name.
UTC(k)	National realization of Coordinated Universal Time
Valid Certificate	A Certificate that passes the validation procedure specified in RFC 5280.
Validation Specialists	Someone who performs the information verification duties specified by these Requirements
Validity Period	The period of time measured from the date when the Certificate is issued until the Expiry Date
Verified Accountant Letter	A document meeting the requirements specified in Section 11.11.2 of these Guidelines
Verified Legal Opinion	A document meeting the requirements specified in Section 11.11.1 of these Guidelines
Verified Method of Communication	The use of a telephone number, a fax number, an email address, or postal delivery address, confirmed by the CA in accordance with Section 11.5 of the Guidelines as a reliable way of communicating with the Applicant.
Verified Professional Letter	A Verified Accountant Letter or Verified Legal Opinion
VOID	Voice Over Internet Protocol
WebTrust EV Program	The additional audit procedures specified for CAs that issue EV Certificates by the AICPA/CICA to be used in conjunction with its WebTrust Program for Certification Authorities

WebTrust Program for CAs	The then-current version of the AICPA/CICA WebTrust Program for Certification Authorities
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.
Wildcard Certificate	A Certificate containing an asterisk (*) in the left-most position of any of the Subject Fully-Qualified Domain Names contained in the Certificate
Wildcard Domain Name	A Domain Name consisting of a single asterisk character followed by a single full stop character ("*.") followed by a Fully-Qualified Domain Name
XX	CABF Baseline Requirements, v. 1.0.5, Effective 12-Sep-12, user-assigned as XX, based on ISO 3166-1 country code , was allowed

Table 15 - Acronyms and Definitions

Appendix B: References

- CA/Browser Forum - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates- version 1.4.8 (available at https://cabforum.org/baseline-requirements-documents/)
- CA/Browser Forum - Guidelines For The Issuance And Management Of Extended Validation Certificates – version 1.6.5 (available at https://cabforum.org/extended-validation/)
- ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers.
- ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.
- ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
- 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.
- ISO 21188:2006, Public key infrastructure for financial services -- Practices and policy framework. Network and Certificate System Security Requirements, v.1.0, 1/1/2013.
- NIST SP 800-89, Recommendation for Obtaining Assurances for Digital Signature Applications, http://csrc.nist.gov/publications/nistpubs/800-89/SP-800-89_November2006.pdf .
- RFC2119, Request for Comments: 2119, Key words for use in RFCs to Indicate Requirement Levels, Bradner, March 1997.
- RFC2527, Request for Comments: 2527, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, March 1999.
- RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.
- RFC3912, Request for Comments: 3912, WHOIS Protocol Specification, Daigle, September 2004.
- RFC4366, Request for Comments: 4366, Transport Layer Security (TLS) Extensions, Blake-Wilson, et al, April 2006.
- RFC5019, Request for Comments: 5019, The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments, A. Deacon, et al, September 2007.
- RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
- RFC6844, Request for Comments: 6844, DNS Certification Authority Authorization (CAA) Resource Record, Hallam-Baker, Stradling, January 2013.
- RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.
- RFC7482, Request for Comments: 7482, Registration Data Access Protocol (RDAP) Query Format, Newton, et al, March 2015.
- WebTrust for Certification Authorities , SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf .
- X.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

Appendix C: EV Verification Requirements

1. General Overview

1.1. Verification Requirements – Overview

Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, this Appendix and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

i. Verify Applicant's existence and identity, including;

(A) Verify the Applicant's legal existence and identity (as more fully set forth in Item 2 herein),
(B) Verify the Applicant's physical existence (business presence at a physical address), and
(C) Verify the Applicant's operational existence (business activity).

ii. Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;

iii. Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;

iv. Verify the Applicant's authorization for the EV Certificate, including;

(A) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
(B) Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
(C) Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

1.2. Acceptable Methods of Verification – Overview

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subItens below. The Acceptable Methods of Verification set forth in each of Itens 2 through 14 (which usually include alternatives) are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

2. Verification of Applicant's Legal Existence and Identity

2.1. Verification Requirements

To verify the Applicant's legal existence and identity, the CA MUST do the following.

(1) **Private Organization Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized entity, in existence and validly formed (e.g., incorporated) with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration, and not designated on the records of the Incorporating or Registration Agency by labels such as "inactive", "invalid", "not current", or the equivalent.
(B) **Organization Name:** Verify that the Applicant's formal legal name as recorded with the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** Obtain the specific Registration Number assigned to the Applicant by the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Where the Incorporating or Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.
(D) **Registered Agent:** Obtain the identity and address of the Applicant's Registered Agent or Registered Office (as applicable in the Applicant's Jurisdiction of Incorporation or Registration).

(2) **Government Entity Subjects**

(A) **Legal Existence:** Verify that the Applicant is a legally recognized Government Entity, in existence in the political subdivision in which such Government Entity operates.

(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of incorporation, registration, or formation, or the identifier for the legislative act that created the Government Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is a Government Entity.

(3) **Business Entity Subjects**
(A) **Legal Existence:** Verify that the Applicant is engaged in business under the name submitted by the Applicant in the Application.
(B) **Organization Name:** Verify that the Applicant's formal legal name as recognized by the Registration Agency in the Applicant's Jurisdiction of Registration matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** Attempt to obtain the specific unique Registration Number assigned to the Applicant by the Registration Agency in the Applicant's Jurisdiction of Registration. Where the Registration Agency does not assign a Registration Number, the CA SHALL obtain the Applicant's date of Registration.
(D) **Principal Individual:** Verify the identity of the identified Principal Individual.

(4) **Non-Commercial Entity Subjects (International Organizations)**
(A) **Legal Existence:** Verify that the Applicant is a legally recognized International Organization Entity.
(B) **Entity Name:** Verify that the Applicant's formal legal name matches the Applicant's name in the EV Certificate Request.
(C) **Registration Number:** The CA MUST attempt to obtain the Applicant's date of formation, or the identifier for the legislative act that created the International Organization Entity. In circumstances where this information is not available, the CA MUST enter appropriate language to indicate that the Subject is an International Organization Entity.

2.2. Acceptable Method of Verification

(1) **Private Organization Subjects:** Unless verified under subItem (6), all Itens listed in Item 2.1(1) MUST be verified directly with, or obtained directly from, the Incorporating or Registration Agency in the Applicant's Jurisdiction of Incorporation or Registration. Such verification MAY be through use of a Qualified Government Information Source operated by, or on behalf of, the Incorporating or Registration Agency, or by direct contact with the Incorporating or Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Incorporating or Registration Agency, or from a Qualified Independent Information Source.

(2) **Government Entity Subjects:** Unless verified under subItem (6), all Itens listed in Item 2.1(2) MUST either be verified directly with, or obtained directly from, one of the following: (i) a Qualified Government Information Source in the political subdivision in which such Government Entity operates; (ii) a superior governing Government Entity in the same political subdivision as the Applicant (e.g. a Secretary of State may verify the legal existence of a specific State Department), or (iii) from a judge that is an active member of the federal, state or local judiciary within that political subdivision.
Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an Attorney as set forth in Item 1.
Such verification MAY be by direct contact with the appropriate Government Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a Qualified Independent Information Source.

(3) **Business Entity Subjects:** Unless verified under subItem (6), Itens listed in Item 2.1(3) (A) through (C) above, MUST be verified directly with, or obtained directly from, the Registration Agency in the Applicant's Jurisdiction of Registration. Such verification MAY be performed by means of a Qualified Government Information Source, a Qualified Governmental Tax Information Source, or by direct contact with the Registration Agency in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from the Qualified Government Information Source, Qualified Governmental Tax Information Source or Registration Agency, or from a Qualified Independent Information Source. In addition, the CA MUST validate a Principal Individual associated with the Business Entity pursuant to the requirements in subItem (4), below.

(4) **Principal Individual:** A Principal Individual associated with the Business Entity MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the Registration Agency, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of face-to-face validation procedures. Where no face-to-face validation was conducted by the Registration Agency, or the Registration Agency's face-to-face validation procedure does not satisfy these requirements, the CA SHALL perform face-to-face validation.

(A) **Face-To-Face Validation:** The face-to-face validation MUST be conducted before either an employee of the CA, a Latin Notary, a Notary (or equivalent in the Applicant's jurisdiction), a Lawyer, or Accountant (Third-Party Validator). The Principal Individual(s) MUST present the following documentation (Vetting Documents) directly to the Third-Party Validator:

(i) A Personal Statement that includes the following information:

1. Full name or names by which a person is, or has been, known (including all other names used);
2. Residential Address at which he/she can be located;
3. Date of birth; and
4. An affirmation that all of the information contained in the Certificate Request is true and correct.

(ii) A current signed government-issued identification document that includes a photo of the Individual and is signed by the Individual such as:

1. A passport;
2. A driver's license;
3. A personal identification card;
4. A concealed weapons permit; or
5. A military ID.

(iii) At least two secondary documentary evidences to establish his/her identity that include the name of the Individual, one of which MUST be from a financial institution.

1. Acceptable financial institution documents include:
   a. A major credit card, provided that it contains an expiration date and it has not expired'
   b. A debit card from a regulated financial institution, provided that it contains an expiration date and it has not expired,
   c. A mortgage statement from a recognizable lender that is less than six months old,
   d. A bank statement from a regulated financial institution that is less than six months old.
2. Acceptable non-financial documents include:
   a. Recent original utility bills or certificates from a utility company confirming the arrangement to pay for the services at a fixed address (not a mobile/cellular telephone bill),
   b. A copy of a statement for payment of a lease, provided that the statement is dated within the past six months,
   c. A certified copy of a birth certificate,
   d. A local authority tax bill for the current year,
   e. A certified copy of a court order, such as a divorce certificate, annulment papers, or adoption papers.

The Third-Party Validator performing the face-to-face validation MUST:

(i) Attest to the signing of the Personal Statement and the identity of the signer; and

(ii) Identify the original Vetting Documents used to perform the identification. In addition, the Third-Party Validator MUST attest on a copy of the current signed government-issued photo identification document that it is a full, true, and accurate reproduction of the original.

(B) **Verification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), lawyer, or accountant in the jurisdiction of the Individual's residency, and that the Third-Party Validator actually did perform the services and did attest to the signature of the Individual.

(C) **Cross-checking of Information:** The CA MUST obtain the signed and attested Personal Statement together with the attested copy of the current signed government-issued photo identification document. The CA MUST review the documentation to determine that the information is consistent, matches the information in the application, and identifies the Individual. The CA MAY rely on electronic copies of this documentation, provided that:

(i) the CA confirms their authenticity (not improperly modified when compared with the underlying original) with the Third-Party Validator; and
(ii) electronic copies of similar kinds of documents are recognized as legal substitutes for originals under the laws of the CA's jurisdiction.

(5) **Non-Commercial Entity Subjects (International Organization):** Unless verified under subItem (6), all Itens listed in Item 2.1(4) MUST be verified either:

(A) With reference to the constituent document under which the International Organization was formed; or
(B) Directly with a signatory country's government in which the CA is permitted to do business. Such verification may be obtained from an appropriate government agency or from the laws of that country, or by verifying that the country's government has a mission to represent it at the International Organization; or
(C) Directly against any current list of qualified entities that the CA/Browser Forum may maintain at www.cabforum.org.
(D) In cases where the International Organization applying for the EV Certificate is an organ or agency - including a non-governmental organization of a verified International Organization, then the CA may verify the International Organization Applicant directly with the verified umbrella International Organization of which the Applicant is na organ or agency.

(6) The CA may rely on a Verified Professional Letter to establish the Applicant's information listed in (1)-(5) above if

(i) the Verified Professional Letter includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act, and
(ii) the CA confirms the Applicant's organization name specified in the Verified Professional Letter with a QIIS or QGIS.

3. Verification of Applicant's Legal Existence and Identity – Assumed Name

3.1. Verification Requirements

If, in addition to the Applicant's formal legal name, as recorded with the applicable Incorporating Agency or Registration.
Agency in the Applicant's Jurisdiction of Incorporation or Registration, the Applicant's identity, as asserted in the EV Certificate, is to contain any assumed name (also known as "doing business as", "DBA", or "d/b/a" in the US, and "trading as" in the UK) under which the Applicant conducts business, the CA MUST verify that: (i) the Applicant has registered its use of the assumed name with the appropriate government agency for such filings in the jurisdiction of its Place of Business (as verified in accordance with this Appendix), and (ii) that such filing continues to be valid.

3.2. Acceptable Method of Verification

To verify any assumed name under which the Applicant conducts business:
(1) The CA MAY verify the assumed name through use of a Qualified Government Information Source operated by, or on behalf of, an appropriate government agency in the jurisdiction of the Applicant's Place of Business, or by direct contact with such government agency in person or via mail, e-mail, Web address, or telephone; or
(2) The CA MAY verify the assumed name through use of a Qualified Independent Information Source provided that the QIIS has verified the assumed name with the appropriate government agency.
(3) The CA MAY rely on a Verified Professional Letter that indicates the assumed name under which the Applicant conducts business, the government agency with which the assumed name is registered, and that such filing continues to be valid.

4. Verification of Applicant's Physical Existence

4.1. Address of Applicant's Place of Business

(1) **Verification Requirements:** To verify the Applicant's physical existence and business presence, the CA MUST verify that the physical address provided by the Applicant is an address where the Applicant or a Parent/Subsidiary Company conducts business operations (not, for example, a mail drop or P.O. box, or 'care of'

(C/O) address, such as an address for an agent of the Organization), and is the address of the Applicant's Place of Business.

(2) **Acceptable Methods of Verification**
(A) **Place of Business in the Country of Incorporation or Registration**
(i) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and whose Place of Business is NOT the same as that indicated in the relevant Qualified Government Information Source used in Item 2 to verify legal existence:
(1) For Applicants listed at the same Place of Business address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, the CA MUST confirm that the Applicant's address, as listed in the EV Certificate Request, is a valid business address for the Applicant or a Parent/Subsidiary Company by reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's representation that such address is its Place of Business;
(2) For Applicants who are not listed at the same Place of Business address in the current version of either at least one QIIS or QTIS, the CA MUST confirm that the address provided by the Applicant in the EV Certificate Request is the Applicant's or a Parent/Subsidiary Company's business address, by obtaining documentation of a site visit to the business address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:
(a) Verify that the Applicant's business is located at the exact address stated in the EV Certificate Request (e.g., via permanent signage, employee confirmation, etc.),
(b) Identify the type of facility (e.g., office in a commercial building, private residence, storefront, etc.) and whether it appears to be a permanent business location,
(c) Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant,
(d) Indicate whether there is evidence that the Applicant is conducting ongoing business activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.), and
(e) Include one or more photos of (i) the exterior of the site (showing signage indicating the Applicant's name, if present, and showing the street address if possible), and (ii) the interior reception area or workspace.
(3) For all Applicants, the CA MAY alternatively rely on a Verified Professional Letter that indicates the address of the Applicant's or a Parent/Subsidiary Company's Place of Business and that business operations are conducted there.
(4) For Government Entity Applicants, the CA MAY rely on the address contained in the records of the QGIS in the Applicant's jurisdiction.
(5) For Applicants whose Place of Business is in the same country as the Applicant's Jurisdiction of Incorporation or Registration and where the QGIS used in Item 2 to verify legal existence contains a business address for the Applicant, the CA MAY rely on the address in the QGIS to confirm the Applicant's or a Parent/Subsidiary Company's address as listed in the EV Certificate Request, and MAY rely on the Applicant's representation that such address is its Place of Business.
(B) **Place of Business not in the Country of Incorporation or Registration:** The CA MUST rely on a Verified Professional Letter that indicates the address of the Applicant's Place of Business and that business operations are conducted there.

5. Verified Method of Communication

5.1. Verification Requirements

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the CA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

5.2. Acceptable Methods of Verification

To verify a Verified Method of Communication with the Applicant, the CA MUST:
(A) Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with one of the Applicant's Parent/Subsidiary or Affiliate's Places of Business in: (i) records provided by the applicable phone company; (ii) a QGIS, QTIS, or QIIS; or (iii) a Verified Professional Letter; and

(B) Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

6. Verification of Applicant's Operational Existence

6.1. Verification Requirements

The CA MUST verify that the Applicant has the ability to engage in business by verifying the Applicant's, or Affiliate/Parent/Subsidiary Company's, operational existence. The CA MAY rely on its verification of a Government Entity's legal existence under Item 2 as verification of a Government Entity's operational existence.

6.2. Acceptable Methods of Verification

To verify the Applicant's ability to engage in business, the CA MUST verify the operational existence of the Applicant, or its Affiliate/Parent/Subsidiary Company, by:
(1) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has been in existence for at least three years, as indicated by the records of an Incorporating Agency or Registration Agency;
(2) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company is listed in either a current QIIS or QTIS;
(3) Verifying that the Applicant, Affiliate, Parent Company, or Subsidiary Company has an active current Demand Deposit Account with a Regulated Financial Institution by receiving authenticated documentation of the Applicant's, Affiliate's, Parent Company's, or Subsidiary Company's Demand Deposit Account directly from a Regulated Financial Institution; or
(4) Relying on a Verified Professional Letter to the effect that the Applicant has an active current Demand Deposit Account with a Regulated Financial Institution.

7. Verification of Applicant's Domain Name

7.1. Verification Requirements

(1) For each **Fully-Qualified Domain Name** listed in a Certificate, other than a Domain Name with .onion in the right-most label of the Domain Name, the CA SHALL confirm that, as of the date the Certificate was issued, the Applicant (or the Applicant's Parent Company, Subsidiary Company, or Affiliate, collectively referred to as "Applicant" for the purposes of this Item) either is the Domain Name Registrant or has control over the FQDN using a procedure specified in Section 3.2.2.4.
The CA doesn´t issue a Certificate to a Domain Name with .onion in the right-most label of the Domain Name.
(2) **Mixed Character Set Domain Names:** The CA doesn´t issue a Certificate to a Domain Name with .onion in the right-most label of the Domain Name.

8. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

8.1. Verification Requirements

For both the Contract Signer and the Certificate Approver, the CA MUST verify the following.
(1) **Name, Title and Agency:** The CA MUST verify the name and title of the Contract Signer and the Certificate Approver, as applicable. The CA MUST also verify that the Contract Signer and the Certificate Approver are agentes representing the Applicant.
(2) **Signing Authority of Contract Signer:** The CA MUST verify that the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.
(3) **EV Authority of Certificate Approver:** The CA MUST verify, through a source other than the Certificate Approver him- or herself, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the EV Certificate Request:

(A) Submit, and, if applicable, authorize a Certificate Requester to submit, the EV Certificate Request on behalf of the Applicant; and
(B) Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the EV Certificate; and
(C) Approve EV Certificate Requests submitted by a Certificate Requester.

8.2. Acceptable Methods of Verification – Name, Title and Agency

Acceptable methods of verification of the name, title, and agency status of the Contract Signer and the Certificate Approver include the following.

(1) **Name and Title:** The CA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable assurance that a person claiming to act in such a role is in fact the named person designated to act in such role.

(2) **Agency:** The CA MAY verify the agency of the Contract Signer and the Certificate Approver by:

(A) Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation that the Contract Signer and/or the Certificate Approver, as applicable, is an employee;

(B) Obtaining an Independent Confirmation From the Applicant (as described in Item 4), or a Verified Professional Letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, is either na employee or has otherwise been appointed as an agent of the Applicant; or

(C) Obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.

The CA MAY also verify the agency of the Certificate Approver via a certification from the Contract Signer (including in a contract between the CA and the Applicant signed by the Contract Signer), provided that the employment or agency status and Signing Authority of the Contract Signer has been verified.

8.3. Acceptable Methods of Verification – Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the EV Authority of the Certificate Approver, as applicable, include:

(1) **Verified Professional Letter:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a Verified Professional Letter;

(2) **Corporate Resolution:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated corporate resolution that confirms that the person has been granted such Signing Authority, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;

(3) **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Item 11.4);

(4) **Contract between CA and Applicant:** The EV Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA and the Applicant that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(5) **Prior Equivalent Authority:** The signing authority of the Contract Signer, and/or the EV authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.

(A) Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA and the Applicant with a legally valid and enforceable seal or handwritten signature and only when the contract was executed more than 90 days prior to the EV Certificate application. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the EV application. Such details MAY include any of the following:

(i) Agreement title,
(ii) Date of Contract Signer's signature,
(iii) Contract reference number, and
(iv) Filing location.

(B) Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the EV Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:

(i) Under contract to the CA, has served (or is serving) as an Enterprise RA for the Applicant, or
(ii) Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the CA MUST have contacted the Certificate Approver by phone at a previously validated phone number or have accepted a signed and notarized letter approving the certificate request.

(6) **QIIS or QGIS**: The Signing Authority of the Contract Signer, and/or the EV Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as a corporate officer, sole proprietor, or other senior official of the Applicant.

(7) **Contract Signer's Representation/Warranty:** Provided that the CA verifies that the Contract Signer is an employee or agent of the Applicant, the CA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:

(A) That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,
(B) That the Subscriber Agreement is a legally valid and enforceable agreement,
(C) That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions,
(D) That serious consequences attach to the misuse of an EV certificate, and
(E) The contract signer has the authority to obtain the digital equivalent of a corporate seal, stamp or officer's signature to establish the authenticity of the company's Web site.
Note: An example of an acceptable representation/warranty appears in Appendix E.

8.4. Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future EV Certificate Requests, then, after the CA:
. Has verified the name and title of the Contract Signer and that he/she is an employee or agent of the Applicant; and
. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Item 8.2.
The CA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise EV Authority with respect to each future EV Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).
Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all EV Certificates issued at the request of, or approved by, such Certificate Approver(s) until such EV Authority is revoked, and MUST include mutually agreed-upon provisions for (i) authenticating the Certificate Approver when EV Certificate Requests are approved, (ii) periodic re-confirmation of the EV Authority of the Certificate Approver, (iii) secure procedures by which the Applicant can notify the CA that the EV Authority of any such Certificate Approver is revoked, and (iv) such other appropriate precautions as are reasonably necessary.

9. Verification of Signature on Subscriber Agreement and EV Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized EV Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The EV Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Item 8.4 of this Appendix. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the EV Certificate Request. In all cases, applicable signatures MUST be a legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or EV Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or EV Certificate Request), that binds the Applicant to the terms of each respective document.

9.1. Verification Requirements

(1) **Signature:** The CA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each EV Certificate Request in a manner that makes it reasonably certain that the person named as the signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.
(2) **Approval Alternative:** In cases where an EV Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the EV Certificate Request by a Certificate Approver in accordance with the requirements of Item 10 can substitute for authentication of the signature of the Certificate Requester on such EV Certificate Request.

9.2. Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:

(1) Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;
(2) A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with this Appendix, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that he/she did sign the applicable document on behalf of the Applicant;
(3) Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate; or
(4) Notarization by a notary, provided that the CA independently verifies that such notary is a legally qualified notary in the jurisdiction of the Certificate Requester or Contract Signer.

10. Verification of Approval of EV Certificate Request

10.1. Verification Requirements

In cases where an EV Certificate Request is submitted by a Certificate Requester, before the CA issues the requested EV Certificate, the CA MUST verify that an authorized Certificate Approver reviewed and approved the EV Certificate Request.

10.2. Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver's approval of an EV Certificate Request include:
(1) Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the EV Certificate Request;
(2) Notifying the Certificate Approver that one or more new EV Certificate Requests are available for review and approval at a designated access-controlled and secure Web site, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site; or
(3) Verifying the signature of the Certificate Approver on the EV Certificate Request in accordance with Item 9 of this Appendix.

11. Verification of Certain Information Sources

11.1. Verified Legal Opinion

(1) **Verification Requirements:** Before relying on a legal opinion submitted to the CA, the CA MUST verify that such legal opinion meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the legal opinion is authored by an independent legal practitioner retained by and representing the Applicant (or an in-house legal practitioner employed by the Applicant) (Legal Practitioner) who is either:

(i) A lawyer (or solicitor, barrister, advocate, or equivalent) licensed to practice law in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains na office or physical facility, or

(ii) A Latin Notary who is currently commissioned or licensed to practice in the country of the Applicant's Jurisdiction of Incorporation or Registration or any jurisdiction where the Applicant maintains an office or physical facility (and that such jurisdiction recognizes the role of the Latin Notary);

(B) **Basis of Opinion:** The CA MUST verify that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Legal Opinion are based on the Legal Practitioner's stated familiarity with the relevant facts and the exercise of the Legal Practitioner's professional judgment and expertise;

(C) **Authenticity:** The CA MUST confirm the authenticity of the Verified Legal Opinion.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Legal Opinion are:

(A) **Status of Author:** The CA MUST verify the professional status of the author of the legal opinion by directly contacting the authority responsible for registering or licensing such Legal Practitioner(s) in the applicable jurisdiction;

(B) **Basis of Opinion:** The text of the legal opinion MUST make it clear that the Legal Practitioner is acting on behalf of the Applicant and that the conclusions of the legal opinion are based on the Legal

Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise. The legal opinion MAY also include disclaimers and other limitations customary in the Legal Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Legal Practitioner, should the legal opinion prove to be erroneous. An acceptable form of legal opinion is attached as Appendix D;

(C) **Authenticity:** To confirm the authenticity of the legal opinion, the CA MUST make a telephone call or send a copy of the legal opinion back to the Legal Practitioner at the address, phone number, facsimile, or (if available) email address for the Legal Practitioner listed with the authority responsible for registering or licensing such Legal Practitioner, and obtain confirmation from the Legal Practitioner or the Legal Practitioner's assistant that the legal opinion is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Legal Practitioner in records provided by the applicable phone company, QGIS, or QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Item 11.1(2)(A), no further verification of authenticity is required.

11.2. Verified Accountant Letter

(1) **Verification Requirements:** Before relying on an accountant letter submitted to the CA, the CA MUST verify that such accountant letter meets the following requirements:

(A) **Status of Author:** The CA MUST verify that the accountant letter is authored by an Accounting Practitioner retained or employed by the Applicant and licensed within the country of the Applicant's Jurisdiction of Incorporation, Jurisdiction of Registration, or country where the Applicant maintains an office or physical facility.

Verification of license MUST be through the member organization or regulatory organization in the Accounting Practitioner's country or jurisdiction that is appropriate to contact when verifying an accountant's license to practice in that country or jurisdiction. Such country or jurisdiction MUST have an accounting standards body that maintains full membership status with the International Federation of Accountants.

(B) **Basis of Opinion:** The CA MUST verify that the Accounting Practitioner is acting on behalf of the Applicant and that the conclusions of the Verified Accountant Letter are based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the Accounting Practitioner's professional judgment and expertise;

(C) **Authenticity:** The CA MUST confirm the authenticity of the Verified Accountant Letter.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for a Verified Accountant Letter are listed here.

(A) **Status of Author:** The CA MUST verify the professional status of the author of the accountant letter by directly contacting the authority responsible for registering or licensing such Accounting Practitioners in the applicable jurisdiction.

(B) **Basis of Opinion:** The text of the Verified Accountant Letter MUST make clear that the Accounting Practitioner is acting on behalf of the Applicant and that the information in the letter is based on the Accounting Practitioner's stated familiarity with the relevant facts and the exercise of the practitioner's professional judgment and expertise.

The Verified Accountant Letter MAY also include disclaimers and other limitations customary in the Accounting Practitioner's jurisdiction, provided that the scope of the disclaimed responsibility is not so great as to eliminate any substantial risk (financial, professional, and/or reputational) to the Accounting Practitioner, should the Verified Accountant Letter prove to be erroneous. Acceptable forms of Verified Accountant Letter are attached as Appendix C.

(C) **Authenticity:** To confirm the authenticity of the accountant's opinion, the CA MUST make a telephone call or send a copy of the Verified Accountant Letter back to the Accounting Practitioner at the address, phone number, facsimile, or (if available) e-mail address for the Accounting Practitioner listed with the authority responsible for registering or licensing such Accounting Practitioners and obtain confirmation from the Accounting Practitioner or the Accounting Practitioner's assistant that the accountant letter is authentic. If a phone number is not available from the licensing authority, the CA MAY use the number listed for the Accountant in records provided by the applicable phone company, QGIS, or QIIS.

In circumstances where the opinion is digitally signed, in a manner that confirms the authenticity of the document and the identity of the signer, as verified by the CA in Item 11.2(2)(A), no further verification of authenticity is required.

11.3. Face-to-Face Validation

(1) **Verification Requirements:** Before relying on face-to-face vetting documents submitted to the CA, the CA MUST verify that the Third-Party Validator meets the following requirements:

(A) **Qualification of Third-Party Validator:** The CA MUST independently verify that the Third-Party Validator is a legally-qualified Latin Notary or Notary (or legal equivalent in the Applicant's jurisdiction), Lawyer, or Accountant in the jurisdiction of the individual's residency;

(B) **Document Chain of Custody:** The CA MUST verify that the Third-Party Validator viewed the Vetting Documents in a face-to-face meeting with the individual being validated;

(C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the attestation and vetting documents.

(2) **Acceptable Methods of Verification:** Acceptable methods of establishing the foregoing requirements for vetting documents are:

(A) **Qualification of Third-Party Validator:** The CA MUST verify the professional status of the Third-Party Validator by directly contacting the authority responsible for registering or licensing such Third-Party Validators in the applicable jurisdiction;

(B) **Document Chain of Custody:** The Third-Party Validator MUST submit a statement to the CA which attests that they obtained the Vetting Documents submitted to the CA for the individual during a face-to-face meeting with the individual;

(C) **Verification of Attestation:** If the Third-Party Validator is not a Latin Notary, then the CA MUST confirm the authenticity of the vetting documents received from the Third-Party Validator. The CA MUST make a telephone call to the Third-Party Validator and obtain confirmation from them or their assistant that they performed the face-to-face validation. The CA MAY rely upon self-reported information obtained from the Third-Party Validator for the sole purpose of performing this verification process. In circumstances where the attestation is digitally signed, in a manner that confirms the authenticity of the documents, and the identity of the signer as verified by the CA in Item 11.3(1)(A), no further verification of authenticity is required.

11.4. Independent Confirmation From Applicant

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

(A) Received by the CA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the appropriate authority to confirm such a fact, and who represents that he/she has confirmed such fact;

(B) Received by the CA in a manner that authenticates and verifies the source of the confirmation; and

(C) Binding on the Applicant.

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

(1) **Confirmation Request:** The CA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:

(A) **Addressee:** The Confirmation Request MUST be directed to:

(i) A position within the Applicant's organization that qualifies as a Confirming Person (e.g., Secretary, President, CEO, CFO, COO, CIO, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, Verified Legal Opinion, Verified Accountant Letter, or by contacting the Applicant using a Verified Method of Communication; or

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

(iii) A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's Human Resources Department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with this Appendix).

(B) **Means of Communication:** The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

(i) By paper mail addressed to the Confirming Person at:

(1) The address of the Applicant's Place of Business as verified by the CA in accordance with this Appendix, or

(2) The business address for such Confirming Person specified in a current QGIS, QTIS, QIIS, Verified Professional Letter, or
(3) The address of the Applicant's Registered Agent or Registered Office listed in the official records of the Jurisdiction of Incorporation, or

(ii) By e-mail addressed to the Confirming Person at the business e-mail address for such person listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter; or
(iii) By telephone call to the Confirming Person, where such person is contacted by calling the main phone number of the Applicant's Place of Business (verified in accordance with this Appendix) and asking to speak to such person, and a person taking the call identifies him- or herself as such person; or
(iv) By facsimile to the Confirming Person at the Place of Business. The facsimile number must be listed in a current QGIS, QTIS, QIIS, Verified Legal Opinion, or Verified Accountant Letter. The cover page must be clearly addressed to the Confirming Person.

(2) **Confirmation Response:** The CA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the CA by telephone, by e-mail, or by paper mail, so long as the CA can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

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

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

11.5. Qualified Independent Information Source

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if the CA determines that:
(1) Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and
(2) The database provider updates its data on at least an annual basis.

The CA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use. The CA SHALL NOT use any data in a QIIS that the CA knows is (i) self-reported and (ii) not verified by the QIIS as accurate. Databases in which the CA or its owners or affiliated companies maintain a controlling interest, or in which any Registration Authorities or subcontractors to whom the CA has outsourced any portion of the vetting process (or their owners or affiliated companies) maintain any ownership or beneficial interest, do not qualify as a QIIS.

11.6. Qualified Government Information Source

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Government Entity, the reporting of data is required by law, and false or misleading reporting is punishable with criminal or civil penalties. Nothing in this Appendix shall prohibit the use of third-party vendors to obtain the information from the Government Entity provided that the third party obtains the information directly from the Government Entity.

11.7. Qualified Government Tax Information Source

A Qualified Government Tax Information Source is a Qualified Government Information Source that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in the United States).

12. Other Verification Requirements

12.1. High Risk Status

The High Risk Certificate requirements of Item 4.2.1 of the Baseline Requirements apply equally to EV Certificates.

12.2. Denied Lists and Other Legal Black Lists

(1) **Verification Requirements:** The CA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the 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 country of the CA's jurisdiction(s) of operation; or

(B) Has its Jurisdiction of Incorporation, Registration, or Place of Business in any country with which the laws of the CA's jurisdiction prohibit doing business.

The CA MUST NOT issue any EV Certificate to the Applicant if either the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction of Incorporation or Registration or Place of Business is on any such list.

(2) **Acceptable Methods of Verification:** The CA MUST take reasonable steps to verify with the following lists and regulations:

(A) If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:

(i) BIS Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp

(ii) BIS Denied Entities List - http://www.bis.doc.gov/Entities/Default.htm

(iii) US Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/ofac/t11sdn.pdf

(iv) US Government export regulations

(B) If the CA has operations in any other country, the CA MUST take reasonable steps to verify with all equivalente denied lists and export regulations (if any) in such other country.

12.3. Parent/Subsidiary/Affiliate Relationship

A CA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under Item 4.1, 5, 6.1, or 7.1, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:

(1) QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;

(2) Independent Confirmation from the Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between na Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Item 11.4);

(3) Contract between CA and Parent, Subsidiary, or Affiliate: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA and the Parent, Subsidiary, or Affiliate that designates the Certificate Approver with such EV Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;

(4) Verified Professional Letter: A CA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Professional Letter; or

(5) Corporate Resolution: A CA MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated corporate resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate corporate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

13. Final Cross-Correlation and Due Diligence

Except for Enterprise EV Certificates:

(1) The results of the verification processes and procedures outlined in this Appendix are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the CA MUST have a person who is not responsible for the collection of information review all of the information and

documentation assembled in support of the EV Certificate application and look for discrepancies or other details requiring further explanation.
(2) The CA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, Qualified Independent Information Sources, and/or other sources of information, as necessary, to resolve those discrepancies or details that require further explanation.
(3) The CA MUST refrain from issuing an EV Certificate until the entire corpus of information and documentation assembled in support of the EV Certificate Request is such that issuance of the EV Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate,. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the EV Certificate Request and SHOULD notify the Applicant accordingly.
(4) In the case where some or all of the documentation used to support the application is in a language other than the CA's normal operating language, the CA or its Affiliate MUST perform the requirements of this Final Cross-Correlation and Due Diligence Item using employees under its control and having appropriate training, experience, and judgment in confirming organizational identification and authorization and fulfilling all qualification requirements contained in Item 14.1 of this Appendix. When employees under the control of the CA do not possess the language skills necessary to perform the Final Cross-Correlation and Due Diligence a CA MAY:

(A) Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
(B) When the CA has utilized the services of an RA, the CA MAY rely on the language skills of the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with Item 13, SubItens (1), (2) and (3). Notwithstanding the foregoing, prior to issuing the EV Certificate, the CA MUST review the work completed by the RA and determine that all requirements have been met; or
(C) When the CA has utilized the services of an RA, the CA MAY rely on the RA to perform the Final Cross-Correlation and Due Diligence, provided that the RA complies with this Item and is subjected to the Audit Requirements.

In the case of Enterprise EV Certificates to be issued in compliance with the requirements of Item 14.2 of this Appendix, the Enterprise RA MAY perform the requirements of this Final Cross-Correlation and Due Diligence Item.

14. Requirements for Re-use of Existing Documentation

For each EV Certificate Request, including requests to renew existing EV Certificates, the CA MUST perform all authentication and verification tasks required by this Appendix to ensure that the request is properly authorized by the Applicant and that the information in the EV Certificate is still accurate and valid. This Item sets forth the age limitations on for the use of documentation collected by the CA.

14.1. Validation For Existing Subscribers

If an Applicant has a currently valid EV Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of:
(1) The Principal Individual verified under Item 2.2 (4) if the individual is the same person as verified by the CA in connection with the Applicant's previously issued and currently valid EV Certificate;
(2) The Applicant's Place of Business under Item 4.1;
(3) The Applicant's Verified Method of Communication required by Item 5 but still MUST perform the verification required by Item 5.2(B);
(4) The Applicant's Operational Existence under Item 6;
(5) The Name, Title, Agency and Authority of the Contract Signer, and Certificate Approver, under Item 8; and
(6) The Applicant's right to use the specified Domain Name under Item 7, provided that the CA verifies that the WHOIS record still shows the same registrant as when the CA verified the specified Domain Name for the initial EV Certificate.

14.2. Re-issuance Requests

A CA may rely on a previously verified certificate request to issue a replacement certificate, so long as the certificate being referenced was not revoked due to fraud or other illegal conduct, if:
(1) The expiration date of the replacement certificate is the same as the expiration date of the EV Certificate that is being replaced, and
(2) The Subject Information of the Certificate is the same as the Subject in the EV Certificate that is being replaced.

14.3. Age of Validated Data

(1) Except for reissuance of an EV Certificate under Item 14.2 and except when permitted otherwise in Item 14.1, the age of all data used to support issuance of an EV Certificate (before revalidation is required) SHALL NOT exceed the following limits:

(A) Legal existence and identity – thirteen months;

(B) Assumed name – thirteen months;

(C) Address of Place of Business – thirteen months;

(D) Verified Method of Communication – thirteen months;

(E) Operational existence – thirteen months;

(F) Domain Name – thirteen months;

(G) Name, Title, Agency, and Authority – thirteen months, unless a contract between the CA and the Applicant specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of EV roles until revoked by the Applicant or CA, or until the contract expires or is terminated.

(2) The thirteen-month period set forth above SHALL begin to run on the date the information was collected by the CA.

(3) The CA MAY reuse a previously submitted EV Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single EV Certificate Request in support of multiple EV Certificates containing the same Subject to the extent permitted under Itens 9 and 10.

(4) The CA MUST repeat the verification process required in this Appendix for any information obtained outside the time limits specified above except when permitted otherwise under Item 14.1.

Appendix D: Sample Attorney Opinions Confirming Specified Information (Informative)

[Law Firm Letterhead]
[Date]
To: ***[Name of Issuing Certification Authority]***
[Address / fax number of Issuing CA – may be sent by fax or emailattachment]
Re: EV Certificate Request No. ***[CA Reference Number]***
Client: ***[Exact company name of Client[11]]***
Client Representative: ***[Exact name of Client Representative who signed the Application[12]]***
Application Date: ***[Insert date of Client's Application to the Issuing CA,]***

This firm represents *[exact company name of Client]**1*** ("Client"), who has submitted the Applicationto you dated as of the Application Date shown above ("Application"). We have been asked by our Client to present you with our opinion as stated in this letter.
[Insert customary preliminary matters for opinion letters in your jurisdiction.]
On this basis, we hereby offer the following opinion:
1. That [exact company name of Client] ("Company") is a duly formed [corporation, LLC, etc.] that is "active," "valid," "current," or the equivalent under the laws of the state/province of [name of governing jurisdiction where Client is incorporated or registered] and is not under any legal disability known to the author of this letter.
2. That Company conducts business under the assumed name or "DBA"*[assumed name of the Applicant]* and has registered such name with the appropriate government agency in the jurisdiction of its place of business below.
3. That *[name of Client's Representative]**2*** has authority to act on behalf of Company to: [*select as appropriate*] (a) provide the information about Company required for issuance of the EV Certificates as contained in the attached Application, (b) request one or more EV Certificates and to designate other persons to request EV Certificates, and (c) agree to the relevant contractual obligations contained in the Subscriber Agreement on behalf of Company.
4. That Company has a physical presence and its place of business is at the following location:
_____

5. That Company can be contacted at its stated place of business at the following telephone number
_____

6. That Company has an active current Demand Deposit Account with a regulated financial institution.
7. That Company has the right to use the following Domain Name in identifying itself on the Internet
_____
[Insert customary limitations and disclaimers for opinion letters in your jurisdiction.

[Name and signature]

[Jurisdiction(s) in which attorney / Latin notary is admitted to practice[13]]

cc: [Send copy to Client*]*

---

[11] This must be the Client's exact corporate name, as registered with the relevant Incorporating Agency in the Client's Jurisdiction of Incorporation. This is the name that will be included in the EV Certificate
[12] If necessary to establish the Client Representative's actual authority, you may rely on a Power of Attorney from an officer of Client who has authority to delegate the authority to the Client Representative
[13] This letter may be issued by in-house counsel for the Client so long as permitted by the rules of your jurisdiction.

Appendix E: Sample Contract Signer's Representation/Warranty (Informative)

A CA may rely on the Contract Signer's authority to enter into the Subscriber Agreement using a representation/warranty executed by the Contract Signer. An example of an acceptable warranty is as follows: [CA] and Applicant are entering into a legally valid and enforceable Subscriber Agreement that creates extensive obligations on Applicant. An EV Certificate serves as a form of digital identity for Applicant. The loss or misuse of this identity can result in great harm to the Applicant. By signing this Subscriber Agreement, the contract signer acknowledges that they have the authority to obtain the digital equivalent of a company stamp, seal, or (where applicable) officer's signature to establish the authenticity of the company's website, and that [Applicant name] is responsible for all uses of its EV Certificate. By signing this Agreement on behalf of [Applicant name], the contract signer represents that the contract signer (i) is acting as an authorized representative of [Applicant name], (ii) is expressly authorized by [Applicant name] to sign Subscriber Agreements and approve EV Certificate requests on Applicant's behalf, and (iii) has confirmed Applicant's right to use the domain(s) to be included in EV Certificates.

Appendix F: Issuance of Certificates for .onion Domain Names

Not applicable.

Appendix G: EV Code Signing Verification Requirements

1. General Overview

1.1. Verification Requirements – Overview

Before issuing an EV Code Signing Object, the CA MUST ensure that all Subject organization information to be included in the EV Code Signing Object conforms to the requirements of, and is verified in accordance with, this Appendix and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

i. Verify Applicant's existence and identity, including;

(A) Verify the Applicant's legal existence and identity (as more fully set forth in Item 2 herein),
(B) Verify the Applicant's physical existence (business presence at a physical address), and
(C) Verify the Applicant's operational existence (business activity).

ii.. Verify the Applicant's authorization for the EV Code Signing Certificate, including;

(A) Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
(B) Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
(C) Verify that a Certificate Approver has signed or otherwise approved the EV Code Signing Certificate Request.

An EV Timestamp Authority is NOT REQUIRED to validate in any way data submitted to it for time-stamping. It simply adds the time to the data that are presented to it, signs the result and appends its own certificate.

1.2. Acceptable Methods of Verification – Overview

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in the subItens below. The Acceptable Methods of Verification set forth in each of Itens 2 through 9. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

2. Verification of Applicant's Legal Existence and Identity

As described at Appendix C, item 2.

3. Verification of Applicant's Legal Existence and Identity – Assumed Name

As described at Appendix C, item 3.

4. Verification of Applicant's Physical Existence

As described at Appendix C, item 4.

5. Verification of Applicant's Operational Existence

As described at Appendix C, item 6.

6. Verification of Applicant's Domain Name

As described at Appendix C, item 7.

7. Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

As described at Appendix C, item 8.

8. Verification of Signature on Subscriber Agreement and EV Code Signing Certificate Requests

As described at Appendix C, item 9.

9. Verification of Approval of EV Code Signing Certificate Request

As described at Appendix C, item 10.

10. Verification of Certain Information Sources

As described at Appendix C, item 11.

11. Other Verification Requirements

As described at Appendix C, item 12.

12. Final Cross-Correlation and Due Diligence

As described at Appendix C, item 13.

13. Requirements for Re-use of Existing Documentation

As described at Appendix C, item 14.

Appendix H – RFC 6844 Errata 5065

The following errata report has been held for document update for RFC6844, "DNS Certification Authority Authorization (CAA) Resource Record".

You may review the report below and at: http://www.rfc-editor.org/errata/eid5065

Status: Held for Document Update
Type: Technical
Reported by: Phillip Hallam-Baker Date Reported: 2017-07-10 Held by: EKR (IESG)

Section: 4
Original Text
Let CAA(X) be the record set returned in response to performing a CAA record query on the label X, P(X) be the DNS label immediately above X in the DNS hierarchy, and A(X) be the target of a CNAME or DNAME alias record specified at the label X.
o If CAA(X) is not empty, R(X) = CAA (X), otherwise
o If A(X) is not null, and R(A(X)) is not empty, then R(X) = R(A(X)), otherwise
o If X is not a top-level domain, then R(X) = R(P(X)), otherwise
o R(X) is empty.

Corrected Text
Let CAA(X) be the record set returned in response to performing a CAA record query on the label X, P(X) be the DNS label immediately above X in the DNS hierarchy, and A(X) be the target of a CNAME or DNAME alias record chain specified at the label X.
o If CAA(X) is not empty, R(X) = CAA (X), otherwise
o If A(X) is not null, and CAA(A(X)) is not empty, then R(X) = CAA(A(X)), otherwise
o If X is not a top-level domain, then R(X) = R(P(X)), otherwise
o R(X) is empty.
Thus, when a search at node X returns a CNAME record, the CA will follow the CNAME record chain to its target. If the target label contains a CAA record, it is returned.
Otherwise, the CA continues the search at the parent of node X.
Note that the search does not include the parent of a target of a CNAME record (except when the CNAME points back to its own path).
To prevent resource exhaustion attacks, CAs SHOULD limit the length of CNAME chains that are accepted. However CAs MUST process CNAME chains that contain 8 or fewer CNAME records.

Appendix I – Abstract Syntax Notation One module for EV certificates

```
CABFSelectedAttributeTypes {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140)
module(4) cabfSelectedAttributeTypes(1) 1}
DEFINITIONS ::=
BEGIN
-- EXPORTS All
IMPORTS
        -- from Rec. ITU-T X.501 | ISO/IEC 9594-2 selectedAttributeTypes, ID, ldap-enterprise
        FROM UsefulDefinitions {joint-iso-itu-t ds(5) module(1) usefulDefinitions(0) 7}

        -- from the X.500 series ub-locality-name, ub-state-name FROM UpperBounds {joint-iso-itu-t ds(5)
        module(1) upperBounds(10) 7}

        -- from Rec. ITU-T X.520 | ISO/IEC 9594-6 DirectoryString{}, CountryName FROM
        SelectedAttributeTypes selectedAttributeTypes;

id-evat-jurisdiction ID ::= {ldap-enterprise 311 ev(60) 2 1}
id-evat-jurisdiction-localityName ID ::= {id-evat-jurisdiction 1}
id-evat-jurisdiction-stateOrProvinceName ID ::= {id-evat-jurisdiction 2}
id-evat-jurisdiction-countryName ID ::= {id-evat-jurisdiction 3}


jurisdictionLocalityName ATTRIBUTE ::= {
        SUBTYPE OF name
        WITH SYNTAX DirectoryString{ub-locality-name}
        LDAP-SYNTAX directoryString.&id
        LDAP-NAME {"jurisdictionL"}
        ID id-evat-jurisdiction-localityName }

jurisdictionStateOrProvinceName ATTRIBUTE ::= {
        SUBTYPE OF name
        WITH SYNTAX DirectoryString{ub-state-name}
        LDAP-SYNTAX directoryString.&id
        LDAP-NAME {"jurisdictionST"} ID id-evat-jurisdiction-stateOrProvinceName }

jurisdictionCountryName ATTRIBUTE ::= {
        SUBTYPE OF name
        WITH SYNTAX CountryName
        SINGLE VALUE TRUE
        LDAP-SYNTAX countryString.&id
        LDAP-NAME {"jurisdictionC"}
        ID id-evat-jurisdiction-countryName }

END
```

Appendix J – DNS CONTACT PROPERTIES

These methods allow domain owners to publish contact information in DNS for the purpose of validating domain control.

J.1. CAA Methods

J.1.1. CAA contactemail Property

SYNTAX: contactemail <rfc6532emailaddress>

The CAA contactemail property takes an email address as its parameter. The entire parameter value MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.

The following is an example where the holder of the domain specified the contact property using an email address.

$ORIGIN example.com.

CAA 0 contactemail "domainowner@example.com"

The contactemail property MAY be critical, if the domain owner does not want CAs who do not understand it to issue certificates for the domain.

J.2. DNS TXT Methods

J.2.1. DNS TXT Record Email Contact

The DNS TXT record MUST be placed on the "_validation-contactemail" subdomain of the domain being validated. The entire RDATA value of this TXT record MUST be a valid email address as defined in RFC 6532 section 3.2, with no additional padding or structure, or it cannot be used.