CERTISIGN CERTIFICATION AUTHORITY CERTIFICATION PRACTICE STATEMENT

VERSION 1.0

JUNE, 6, 2018

Summary

1. INTRODUCTION

This document is CERTISIGN CERTIFICATION AUTHORITY Certification Practice Statement (CERTISIGN CERTIFICATION AUTHORITY CPS). It states the practices that CERTISIGN CERTIFICATION AUTHORITY employs in providing certification services that include, but are not limited to, issuing, managing, revoking, and renewing certificates in accordance with the specific requirements of CERTISIGN TRUST NETWORK Certificate Policies ("CTN CP").

This document is targeted at:

- CERTISIGN TRUST NETWORK PKI service providers who have to operate in terms of their own Certificate Practices (CP) that complies with the requirements laid down by the CPS
- CERTISIGN CERTIFICATION AUTHORITY 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 CPS 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 1.5.7 (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 CPS is applicable to CERTISIGN CERTIFICATION AUTHORITY, who operates as CAs under CERTISIGN TRUST NETWORK CP, issuing end-user subscriber certificates.

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.

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 CERTIFICATION AUTHORITY CERTIFICATION PRACTICE STATEMENT (CERTISIGN CERTIFICATION AUTHORITY CPS).

1.2.1 CABF Policy Identifiers

CERTISIGN CERTIFICATION AUTHORITY OID is defined as 1.3.6.1.4.1.30253.22.

1.2.2 Revision

Version	Description	Adopted
1.0	✓ CERTISIGN CERTIFICATION AUTHORITY creation	06/06/2018

Table 1 - Revision

1.3 PKI Participants

As described at CERTISIGN TRUST NETWORK CP.

1.4 Certificate Usage

CERTISIGN CERTIFICATION AUTHORITY issues certificate to be used by Subscribers to secure websites throught Domain Validation (SSL DV).

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 CERTIFICATION AUTHORITY Policy Management Department (PMD), named as “Normas e Compliance” determines the suitability and applicability of this CPS.

1.5.4 CPS Approval Procedure

Approval of this CPS 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 CPS 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/certisign-ca/certisign-ca-certification-authority.htm

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

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 is responsible for maintaining a publicly accessible online repository, as well as revocation information concerning Certificates it issues.

2.2 Publication of Certificate Information

CERTISIGN maintains 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 CERTIFICATION AUTHORITY CPS,
- CERTISIGN ROOT CERTIFICATION AUTHORITY CPS,
- CERTISIGN TRUST NETWORK CP and 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

As described at CERTISIGN TRUST NETWORK CP.

2.4 Access Controls on Repositories

As described at CERTISIGN TRUST NETWORK CP.

3.1 Naming

Names appearing in Certificates issued under CERTISIGN CERTIFICATION AUTHORITY are authenticated.

3.1.1 Type of Names

CERTISIGN CERTIFICATION AUTHORITY 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)

Table 2 - Distinguished Name Attributes in End User Subscriber Certificates

3.1.1.1 CABF Naming Requirements

Domain 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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

Not applicable.

3.1.2 Need for Names to be Meaningful

CERTISIGN CERTIFICATION AUTHORITY 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.

3.2.1.1. CABF Verification Requirements for EV

Not applicable.

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 CPS 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 CPS and/or CERTISIGN’s internal documents..

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

3.2.2.1. Identity

CERTISIGN SHALL verify the identity and address of the Applicant using

1. documentation provided by the Applicant and
2. 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.

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

Alternatively, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY determines to be reliable.

3.2.2.2. DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY determines to be reliable.

3.2.2.3. Verification of Country

CERTISIGN CERTIFICATION AUTHORITY SHALL verify the country associated with the Subject using one of the following:
(a) information provided by the Domain Name Registrar; or
(b) a method identified in Section 3.2.2.1.

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.
CERTISIGN CERTIFICATION AUTHORITY SHALL confirm that prior to issuance, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY MUST follow its CPS.

Note: (i) Once the FQDN has been validated using this method, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY should define in its CPS the format of Request Tokens it accepts.

Note: (i) Once the FQDN has been validated using this method, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless CERTISIGN CERTIFICATION AUTHORITY 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

Not applicable.

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 CERTIFICATION AUTHORITY 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 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 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.

3.2.2.5. Authentication for an IP Address

For each IP Address listed in a Certificate, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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”.[1]

If a wildcard would fall within the label immediately to the left of a registry-controlled or public sufix[2], CERTISIGN CERTIFICATION AUTHORITY MUST refuse issuance unless the applicant proves its rightful control of the entire

[1] See RFC 6454 Section 8.2 for further explanation

[2] 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,

Domain Namespace e.g. CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY, 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 CERTIFICATION AUTHORITY 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 D). If CERTISIGN CERTIFICATION AUTHORITY issues, they MUST do so within the TTL of the CAA record, or 8 hours, whichever is greater.

This stipulation does not prevent CERTISIGN CERTIFICATION AUTHORITY from checking CAA records at any other time.
When processing CAA records, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY MUST NOT issue a certificate unless either
(1) the certificate request is consistent with the applicable CAA Resource Record set or
(2) an exception specified in CP or CPS applies.

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY or its Affiliates is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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.

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.

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY determines to be reliable, such as a government ID, utility bill, or bank or credit card statement . CERTISIGN CERTIFICATION AUTHORITY MAY rely on the same government-issued ID that was used to verify the Applicant's name.

CERTISIGN CERTIFICATION AUTHORITY 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[3]

3.2.5 Validation of Authority

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

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

Provided that CERTISIGN CERTIFICATION AUTHORITY uses a Reliable Method of Communication, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY deems appropriate.

3.2.5.1. CABF Verification Requirements for SSL Certificates

In SSL certificate issuance process under CA/Browser Forum - Baseline Requirements, CERTISIGN CERTIFICATION AUTHORITY SHALL establish a process that allows an Applicant to specify the individuals who

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

MAY request Certificates. If an Applicant specifies, in writing, the individuals who MAY request a Certificate, then CERTISIGN CERTIFICATION AUTHORITY SHALL NOT accept any certificate requests that are outside this specification. CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY by unilaterally certifying that CA. CAs enabled to interoperate in this way will comply with CERTISIGN CERTIFICATION AUTHORITY CP as supplemented by additional policies when required.

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

- Enters into a contractual agreement with CERTISIGN or an Affiliate
- Operates under a CPS that meets CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY SHALL disclose all Cross Certificates that identify CERTISIGN CERTIFICATION AUTHORITY as the Subject, provided that CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY requires that the Subscriber generate a new key pair to replace the expiring key pair (technically defined as "rekey").

3.3.1 Identification and Authentication for Routine Re-key

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

CERTISIGN CERTIFICATION AUTHORITY requires the same proccess as described at 4.1. section.

3.3.2 Identification and Authentication for Re-key After Revocation

CERTISIGN CERTIFICATION AUTHORITY requires the same proccess as described at 4.1. section.

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.

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.

4.1.2 Certificate Application Processing

CERTISIGN CERTIFICATION AUTHORITY SHALL perform identification and authentication of all required Subscriber information in terms of Section 3.2.

CERTISIGN CERTIFICATION AUTHORITY begins processing certificate applications within a reasonable time of receipt. There is no time stipulation to complete the processing of an application.

A certificate application remains active until rejected.

4.1.2.2 CABF Certificate Application Requirements

4.1.2.2.1 SSL Certificates

Prior to the issuance of a SSL Certificate, CERTISIGN CERTIFICATION AUTHORITY SHALL obtain from the Applicant a certificate request in a form prescribed by CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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.

4.2 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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, CERTISIGN CERTIFICATION AUTHORITY may continue to reuse validation data or documents collected prior to the change, or the validation itself, for the period stated in this CPS 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY into disrepute

4.2.2.1. CABF Requirements for SSL Certificates

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY MUST provide a warning to the applicant that the gTLD MAY soon become resolvable and that, at that time, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTISIGN CERTIFICATION AUTHORITY. CERTISIGN CERTIFICATION AUTHORITY creates and issues a Certificate based on the information in a Certificate Application following approval of such Certificate Application.

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

4.3.1.1 Certificate Transparency

CERTISIGN CERTIFICATION AUTHORITY MAY be compliant with Certificate Transparency requirements. When an CERTISIGN CERTIFICATION AUTHORITY certificate is to be issued, a precertificate is generated and registered in a number of CT-logs. Each CT-log returns a signed certificate timestamp (SCT) as a proof of inclusion.

The precertificate is constructed from the certificate to be issued by adding a special poison extension (OID 1.3.6.1.4.1.11129.2.4.3). The precertificate is signed by the same CA issuing the final certificate.

The SCTs are embedded into the final certificate as a certificate extension (OID 1.3.6.1.4.1.11129.2.4.2).

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.

4.4 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 CERTIFICATION AUTHORITY 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 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 CPS. CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY doesn´t allow certificate renewal.

4.7 Certificate Re-Key

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

CERTISIGN CERTIFICATION AUTHORITY requests the Applicant to submit a new certificate application to issue a new certificate.

4.8 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.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

4.9.1.1. Reasons for Revoking a Subscriber Certificate

Only in the circumstances listed below, will an end-user Subscriber certificate be revoked by CERTISIGN CERTIFICATION AUTHORITY (in behalf of the Subscriber) and published on a CRL.

An end-user Subscriber Certificate is revoked if:
1. The Subscriber requests in writing that CERTISIGN CERTIFICATION AUTHORITY revoke the Certificate;
2. The Subscriber notifies CERTISIGN CERTIFICATION AUTHORITY that the original certificate request was not authorized and does not retroactively grant authorization;
3. CERTISIGN CERTIFICATION AUTHORITY, a AR, a Customer or a Subscriber obtains evidence that the Subscriber'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. CERTISIGN CERTIFICATION AUTHORITY, a RA, a Customer or a Subscriber obtains evidence that the Certificate was misused;
5. CERTISIGN CERTIFICATION AUTHORITY, a RA or a Customer is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
6. CERTISIGN CERTIFICATION AUTHORITY, a RA or a Customer is made aware of any circumstance indicating that use of a FQDN or IP address in the Certificate is no longer legally permitted[4];
7. CERTISIGN CERTIFICATION AUTHORITY, a RA or a Customer is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate FQDN;
8. CERTISIGN CERTIFICATION AUTHORITY, a RA or a Customer is made aware of a material change in the information contained in the Certificate;
9. CERTISIGN CERTIFICATION AUTHORITY, a RA or a Customer is made aware that the Certificate was not issued in accordance with these Requirements or the CERTISIGN CERTIFICATION AUTHORITY CP or CPS;
10. CERTISIGN CERTIFICATION AUTHORITY determines that any of the information appearing in the Certificate is inaccurate or misleading;
11. CERTISIGN CERTIFICATION AUTHORITY ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
12. CERTISIGN CERTIFICATION AUTHORITY right to issue Certificates under these Requirements expires or is revoked or terminated, unless CERTISIGN CERTIFICATION AUTHORITY has made arrangements to continue maintaining the CRL/OCSP Repository;
13. CERTISIGN CERTIFICATION AUTHORITY is made aware of a possible compromise of the Private Key of the Subordinate CA used for issuing the Certificate;
14. Revocation is required by CERTISIGN CERTIFICATION AUTHORITY CP and/or CPS;
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties[5];
16. The Subscriber Agreement with the Subscriber has been terminated;
17. The affiliation between an Enterprise Customer with a Subscriber is terminated or has otherwise ended;

[4] 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] e.g. the CA/Browser Forum might determine that a deprecated cryptographic/ signature algorithm or key size presents an unacceptable risk and that such Certificates SHOULD be revoked and replaced by CAs within a given period of time

18. The Subscriber has not submitted payment when due;
19. The Subscriber identity has not been successfully re-verified in accordance with section 3.3.2; or
20. The continued use of that certificate is harmful to CERTISIGN CERTIFICATION AUTHORITY.

When considering whether certificate usage is harmful to CERTISIGN CERTIFICATION AUTHORITY, a CA and/or RA considers, among other things, the following:

- The nature and number of complaints received
- The identity of the complainant(s)
- Relevant legislation in force
- Responses to the alleged harmful use from the Subscriber

CERTISIGN CERTIFICATION AUTHORITY Subscriber Agreements require end-user Subscribers to immediately notify CERTISIGN of a known or suspected compromise of its private key.

CERTISIGN CERTIFICATION AUTHORITY or a RA MAY also revoke an Administrator Certificate if the Administrator's authority to act as Administrator has been terminated or otherwise has ended.

Subscriber Agreements require end-user Subscribers to immediately notify a AR of a known or suspected compromise of its private key.

4.9.1.1.1 CABF Requirements

CERTISIGN CERTIFICATION AUTHORITY SHALL revoke a Certificate within 24 hours.

4.9.1.2. Reasons for Revoking a Subordinate CA Certificate

Not applicable.

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

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

Prior to the revocation of a Certificate, CERTISIGN CERTIFICATION AUTHORITY 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 the CA.

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

Commercially reasonable steps are taken to process revocation requests without delay.

CERTISIGN CERTIFICATION AUTHORITY begins investigation of a Certificate Problem Report within 24 hours of receipt, and decides whether revocation or other appropriate action is warranted based on at least the following criteria:
1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint[6]; and
4. 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. Relying Parties MAY check Certificate status is by consulting the most recent CRL from CERTISIGN CERTIFICATION AUTHORITY .

4.9.7 CRL Issuance Frequency

CERTISIGN CERTIFICATION AUTHORITY CRL SHALL be issued at least daylly, but also within 1 hour whenever a Certificate is revoked.

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.

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 CERTIFICATION AUTHORITY, or
2. Be signed by an OCSP Responder whose Certificate is signed by CERTISIGN CERTIFICATION AUTHORITY. 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

[6] 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

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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY SHALL update information provided via an Online Certificate Status Protocol at least (i) every 4 days and (ii) within 1 hour after revoking a Certificate.

4.9.11 Other Forms of Revocation Advertisements Available

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

4.9.12 Special Requirements Regarding Key Compromise

CERTISIGN CERTIFICATION AUTHORITY Participants SHALL be notified of an actual or suspected CA private key Compromise using commercially reasonable efforts. CERTISIGN CERTIFICATION AUTHORITY 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.

4.10 Certificate Status Services

4.10.1 Operational Characteristics

The status of public certificates is available via CRL through CERTISIGN CERTIFICATION AUTHORITY (at a URL specified in AC's CPS).

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

4.10.2 Service Availability

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

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

CERTISIGN CERTIFICATION AUTHORITY 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

Not applicable.

4.11 End of Subscription

A subscriber MAY end a subscription for a CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY participant MAY escrow CA, RA or end-user Subscriber private keys.

5. Facility, Management, and Operational Controls

5.1 Physical Controls

CERTISIGN CERTIFICATION AUTHORITY CP has documented detailed procedural control for CAs and RAs to adhere to.

5.2 Procedural Controls

CERTISIGN CERTIFICATION AUTHORITY CP has documented detailed procedural control for CAs and RAs to adhere to.

5.3 Personnel Controls

CERTISIGN CERTIFICATION AUTHORITY CP has documented detailed personnel control and security policies for CAs and RAs to adhere to.

5.4 Audit Logging Procedures

As described at CERTISIGN TRUST NETWORK CP.

5.5 Records Archival

As described at CERTISIGN TRUST NETWORK CP.

5.6 Key Changeover

As described at CERTISIGN TRUST NETWORK CP.

5.7 Compromise and Disaster Recovery

As described at CERTISIGN TRUST NETWORK CP.

5.8 CA or RA Termination

As described at CERTISIGN TRUST NETWORK CP.

5.9 Data Security

As described at CERTISIGN TRUST NETWORK CP.

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.

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

Not applicable.

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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY SHALL revoke all certificates that include the Public Key corresponding to the communicated Private Key.

If CERTISIGN CERTIFICATION AUTHORITY or any of its designated RAs generated the Private Key on behalf of the Subscriber, then CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY Certificate MAY also be downloaded from http://ctn.certisign.com.br/certisign-ca/certisign-ca-certification-authority.htm

CERTISIGN make reasonable effort to the public keys of the CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY.

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 CERTIFICATION AUTHORITY:

- key sizes for end-users: 2048 bit RSA
- digital signaturehash algorithm: SHA-1

6.1.5.1 CABF Requirements for Key Sizes

Subscriber Certificates	Validity period ending on or before 31 Dec 2013	Validity period ending after 31 Dec 2013
Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	1024	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	

* SHA-1 MAY be used with RSA keys in accordance with the criteria defined in Section 7.1.3.
** A Root CA Certificate issued prior to 31 Dec. 2010 with an RSA key size less than 2048 bits MAY still serve as a trust anchor for Subscriber Certificates issued in accordance with these Requirements.
***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

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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 SSL Certificates MUST HAVE digitalSignature, nonRepudiation AND keyEncipherment bits activated.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

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

CERTISIGN recommends that SSL certificates to perform cryptographic operations on a cryptographic module rated at least140-1 level 1 certified cryptographic module or other similar standard used in Brazil.

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

Not applicable.

6.2.3 Private Key Escrow

Private keys are not escrowed escrow for end user subscribers.

6.2.4 Private Key Backup

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

CERTISIGN does not archive copies of Subscriber private keys.

6.2.6 Private Key Transfer Into or From a Cryptographic Module

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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

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

Not applicable.

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

CERTISIGN TRUST NETWORK CAs 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 3 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 3 – 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

Subscriber Certificates MUST have a Validity Period no greater than 825 days.

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 strongly recommends that all Subscribers choose passwords that meet CERTISIGN 's password selection guidelines:

- 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 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

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 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

Not applicable.

6.4.3.2 Activation Data Destruction

Not applicable.

6.5 Computer Security Controls

Not applicable.

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

Not applicable.

6.8 Time-Stamping

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

7. Certificate, CRL, and OCSP Profiles

7.1 Certificate Profile

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY Certificates SHALL contain the basic fields and indicated prescribed values or value constraints in Table 4 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 4- 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 CERTIFICATION AUTHORITY Certificates with the extensions required by this Section.

basicConstraints

Type of Certificate	Subscriber
Required/Optional	optional
criticality field	Must not be TRUE
pathLenConstraint field	--
cA field	

Table 5 -basicConstraints

keyUsage

Type of Certificate	Subscriber
Required/Optional	optional
criticality field	Should be set TRUE or FALSE
bit positions for keyCertSign and cRLSign	If present, they MUST NOT be set
bit positions for digitalSignature	--

Table 6 - keyUsage

certificatePolicies

Type of Certificate	Subscriber
Required/Optional	required
criticality field	SHALL be set to FALSE
certificatePolicies:policyIdentifier - Required/Optional	required
certificatePolicies:policyQualifiers - contents	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 7 - certificatePolicies

ExtendedKeyUsage[7]

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

[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.

Table 8 - ExtendedKeyUsage

cRLDistributionPoints

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

Table 9 - cRLDistributionPoints

authorityInformationAccess

Type of Certificate	Subscriber
Required/Optional	required, with the exception of stapling, which is noted below
criticality field	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].

Table 10 - authorityInformationAccess

Subject Key Identifier

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

Table 11 - Subject Key Identifier

nameConstraints [8]

Type of Certificate	Subscriber
Required/Optional	--
criticality field	--

Table 22 - nameConstraints

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

CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY [10].

[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

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

As described in Section 7.1.4.2.

7.1.2.3 CABF Requirement for Certificate Policies Extension for EV

Not applicable.

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

Not applicable.

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 CERTIFICATION AUTHORITY 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}
- sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}

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 using the SHA-1 hash algorithm.
- 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 CERTIFICATION AUTHORITY 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.

7.1.4.2. Subject Information – Subscriber Certificates

By issuing the Certificate, CERTISIGN CERTIFICATION AUTHORITY 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 CERTIFICATION AUTHORITY 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.

7.1.4.2.1.1. Reserved IP Address or Internal Name

CERTISIGN CERTIFICATION AUTHORITY 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

Not applicable.

7.1.4.2.4. Subject Alternative Name Extension for EV Certificates

Not applicable.

7.1.4.2.5. Subject Distinguished Name Fields for EV Code Signing Certificates

Not applicable.

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

Not applicable.

7.1.5 Name Constraints

When an CERTISIGN CERTIFICATION AUTHORITY certificate is Certificate Transparency compliant, signed certificate timestamp (SCT) are embedded into the certificate extension SignedCertificate-TimestampList (OID 1.3.6.1.4.1.11129.2.4.2), no critical.

7.1.6 Certificate Policy Object Identifier

CERTISIGN CERTIFICATION AUTHORITY OID is defined as 1.3.6.1.4.1.30253.22.

7.1.6.1. Reserved CP Identifiers

Not applicable.

7.1.6.2. Root CA Certificates

Not applicable.

7.1.6.3. Subordinate CA Certificates

Not applicable.

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 CERTIFICATION AUTHORITY 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 this CERTISIGN CERTIFICATION AUTHORITY 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 13 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 13 - 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 SSL Certificates conform to CERTISIGN TRUST NETWORK / Browser Forum Baseline requirements.

OCSP Responses SHALL conform to RFC5019 and either be:

- Signed by CERTISIGN CERTIFICATION AUTHORITY, that issued the Certificates whose revocation status is being checked, or
- Signed by an OCSP Responder whose Certificate is signed by C CERTISIGN CERTIFICATION AUTHORITY. 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

As described at CERTISIGN TRUST NETWORK CP.

8.1 Frequency and Circumstances of Assessment

As described at CERTISIGN TRUST NETWORK CP.

8.2 Identity/Qualifications of Assessor

As described at CERTISIGN TRUST NETWORK CP.

8.3 Assessor's Relationship to Assessed Entity

As described at CERTISIGN TRUST NETWORK CP.

8.4 Topics Covered by Assessment

As described at CERTISIGN TRUST NETWORK CP.

8.5 Actions Taken as a Result of Deficiency

As described at CERTISIGN TRUST NETWORK CP.

8.6 Communications of Results

As described at CERTISIGN TRUST NETWORK CP.

8.7. Self-Audits

As described at CERTISIGN TRUST NETWORK CP.

9. Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance or Renewal Fees

As described at CERTISIGN TRUST NETWORK CP.

9.1.2 Certificate Access Fees

As described at CERTISIGN TRUST NETWORK CP.

9.1.3 Revocation or Status Information Access Fees

As described at CERTISIGN TRUST NETWORK CP.

9.1.4 Fees for Other Services

As described at CERTISIGN TRUST NETWORK CP.

9.1.5 Refund Policy

As described at CERTISIGN TRUST NETWORK CP.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

As described at CERTISIGN TRUST NETWORK CP.

9.2.2 Other Assets

As described at CERTISIGN TRUST NETWORK CP.

9.2.3 Extended Warranty Coverage

As described at CERTISIGN TRUST NETWORK CP.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

As described at CERTISIGN TRUST NETWORK CP.

9.3.2 Information Not Within the Scope of Confidential Information

As described at CERTISIGN TRUST NETWORK CP.

9.3.3 Responsibility to Protect Confidential Information

As described at CERTISIGN TRUST NETWORK CP.

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

As described at CERTISIGN TRUST NETWORK CP.

9.4.2 Information Treated as Private

As described at CERTISIGN TRUST NETWORK CP.

9.4.3 Information Not Deemed Private

As described at CERTISIGN TRUST NETWORK CP.

9.4.4 Responsibility to Protect Private Information

As described at CERTISIGN TRUST NETWORK CP.

9.4.5 Notice and Consent to Use Private Information

As described at CERTISIGN TRUST NETWORK CP.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

As described at CERTISIGN TRUST NETWORK CP.

9.4.7 Other Information Disclosure Circumstances

As described at CERTISIGN TRUST NETWORK CP.

9.5 Intellectual Property Rights

As described at CERTISIGN TRUST NETWORK CP.

9.5.1 Property Rights in Certificates and Revocation Information

As described at CERTISIGN TRUST NETWORK CP.

9.5.2 Property Rights in the CP

As described at CERTISIGN TRUST NETWORK CP.

9.5.3 Property Rights in Names

As described at CERTISIGN TRUST NETWORK CP.

9.5.4 Property Rights in Keys and Key Material

As described at CERTISIGN TRUST NETWORK CP.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

As described at CERTISIGN TRUST NETWORK CP.

9.6.2 RA Representations and Warranties

As described at CERTISIGN TRUST NETWORK CP.

9.6.3 Subscriber Representations and Warranties

As described at CERTISIGN TRUST NETWORK CP.

9.6.4 Relying Party Representations and Warranties

As described at CERTISIGN TRUST NETWORK CP.

9.6.5 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

As described at CERTISIGN TRUST NETWORK CP.

9.8 Limitations of Liability

As described at CERTISIGN TRUST NETWORK CP.

9.8.1 Limitations of Liability for EV

Not applicable.

9.9 Indemnities

9.9.1 Indemnification by Subscribers

As described at CERTISIGN TRUST NETWORK CP.

9.9.2 Indemnification by Relying Parties

As described at CERTISIGN TRUST NETWORK CP.

9.9.3 Indemnification of Application Software Suppliers

As described at CERTISIGN TRUST NETWORK CP.

9.10 Term and Termination

9.10.1 Term

As described at CERTISIGN TRUST NETWORK CP.

9.10.2 Termination

As described at CERTISIGN TRUST NETWORK CP.

9.10.3 Effect of Termination and Survival

As described at CERTISIGN TRUST NETWORK CP.

9.11 Individual Notices and Communications with Participants

As described at CERTISIGN TRUST NETWORK CP.

9.12 Amendments

9.12.1 Procedure for Amendment

As described at CERTISIGN TRUST NETWORK CP.

9.12.2 Notification Mechanism and Period

As described at CERTISIGN TRUST NETWORK CP.

9.12.3 Circumstances under Which OID Must be Changed

As described at CERTISIGN TRUST NETWORK CP.

9.13 Dispute Resolution Provisions

9.13.1 Disputes among CERTISIGN, Affiliates, and Customers

As described at CERTISIGN TRUST NETWORK CP.

9.13.2 Disputes with End-User Subscribers or Relying Parties

As described at CERTISIGN TRUST NETWORK CP.

9.14 Governing Law

As described at CERTISIGN TRUST NETWORK CP.

9.15 Compliance with Applicable Law

As described at CERTISIGN TRUST NETWORK CP.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

Not applicable

9.16.2 Assignment

Not applicable

9.16.3 Severability

As described at CERTISIGN TRUST NETWORK CP.

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 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 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
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, an unauthorized person has had access to it, or there exists a practical technique by which an unauthorized person MAY discover its value. A Private Key is also considered compromised if 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.
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
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
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

Table 14 - 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

Not applicable

APPENDIX D: 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.