Amazon Trust Services Certificate Policy

amazon trust services

Version 1.0.6

Contents

Contents
1 INTRODUCTION
1.1 Overview
1.1.1 Compliance
1.1.2 Types of Certificates
1.1.2.1 CA-Certificates
1.1.2.1.3 Terminus CA-Certificates
1.1.2.1.4 Policy CA-Certificates
1.1.2.1.5 Technically Constrained CA-Certificates
1.1.2.1.6 Unconstrained CA-Certificates
1.1.2.1.7 Root CA-Certificates
1.1.2.1.8 Subordinate CA-Certificates
1.1.2.2 End-Entity Certificates
1.1.2.2.1 Extended Validation TLS Server Authentication Certificates
1.1.2.2.2 Standard Validation TLS Server Authentication Certificates
1.1.2.2.3 Extended Validation Code Signing Certificates
1.1.2.2.4 Standard Validation Code Signing Certificates
1.1.2.2.5 Client Certificates (including Augmented Client Certificates)
1.1.2.2.6 OCSP Signing Certificate
1.1.2.2.7 Time Stamp Authority Certificate
1.1.2.3 Subscriber Certificates
1.2 Document name and identification
1.3 PKI participants
1.3.1 Certification authorities
1.3.2 Registration authorities
1.3.3 Subscribers
1.3.4 Relying parties
1.3.5 Other participants
1.4 Certificate usage
1.4.1 Appropriate certificate uses
1.4.2 Prohibited certificate uses
1.5 Policy administration
1.5.1 Organization administering the document
1.5.2 Contact person
1.5.3 Person determining CPS suitability for the policy
1.5.4 CPS approval procedures
1.6 Definitions and acronyms
1.6.1 Definitions
1.6.2 Acronyms
1.6.3 References
1.6.4 Conventions
2 PUBLICATION AND REPOSITORY RESPONSIBILITIES
2.1 Repositories
2.2 Publication of certification information
2.3 Time or frequency of publication

2.4 Access controls on repositories
3 IDENTIFICATION AND AUTHENTICATION
3.1 Naming
3.1.1 Types of names
3.1.2 Need for names to be meaningful
3.1.3 Anonymity or pseudonymity of subscribers
3.1.4 Rules for interpreting various name forms
3.1.5 Uniqueness of names
3.1.6 Recognition, authentication, and role of trademarks
3.2 Initial identity validation
3.2.1 Method to prove possession of private key
3.2.2 Validation of Domain Authorization or Control
3.2.2.1 Identity
3.2.2.2 DBA/Tradename
3.2.2.3 Verification of Country
3.2.2.4 Validation of Domain Authorization or Control
3.2.2.4.1 Validating the Applicant as a Domain Contact
3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact
3.2.2.4.3 Phone Contact with Domain Contact
3.2.2.4.4 Constructed Email to Domain Contact
3.2.2.4.5 Domain Authorization Document
3.2.2.4.6 Agreed-Upon Change to Website
3.2.2.4.7 DNS Change
3.2.2.4.8 IP Address
3.2.2.4.9 Test Certificate
3.2.2.4.10. TLS Using a Random Number
3.2.2.4.11 Any Other Method
3.2.2.4.12 Validating Applicant as a Domain Contact
3.2.2.5 Authentication for an IP Address
3.2.2.6 Wildcard Domain Validation
3.2.2.7 Data Source Accuracy
3.2.3 Authentication of individual identity
3.2.4 Non-verified subscriber information
3.2.5 Validation of authority
3.2.6 Criteria for interoperation
3.3 Identification and authentication for re-key requests
3.3.1 Identification and authentication for routine re-key
3.3.2 Identification and authentication for re-key after revocation
3.4 Identification and authentication for revocation request
4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS
4.1 Certificate Application
4.1.1 Who can submit a certificate application
4.1.1.1 Private Organization Subjects
4.1.1.2 Government Entity Subjects
4.1.1.3 Business Entity Subjects
4.1.1.4 Non-Commercial Entity Subjects

4.1.2 Enrollment process and responsibilities
4.1.2.1 Applicant roles
4.2 Certificate application processing
4.2.1 Performing identification and authentication functions
4.2.2 Approval or rejection of certificate applications
4.2.3 Time to process certificate applications
4.3 Certificate issuance
4.3.1 CA actions during certificate issuance
4.3.2 Notification to subscriber by the CA of issuance of certificate
4.4 Certificate acceptance
4.4.1 Conduct constituting certificate acceptance
4.4.2 Publication of the certificate by the CA
4.4.3 Notification of certificate issuance by the CA to other entities
4.5 Key pair and certificate usage
4.5.1 Subscriber private key and certificate usage
4.5.2 Relying party public key and certificate usage
4.6 Certificate renewal
4.6.1 Circumstance for certificate renewal
4.6.2 Who may request renewal
4.6.3 Processing certificate renewal requests
4.6.4 Notification of new certificate issuance to subscriber
4.6.5 Conduct constituting acceptance of a renewal certificate
4.6.6 Publication of the renewal certificate by the CA
4.6.7 Notification of certificate issuance by the CA to other entities
4.7 Certificate re-key
4.7.1 Circumstance for certificate re-key
4.7.2 Who may request certification of a new public key
4.7.3 Processing certificate re-keying requests
4.7.4 Notification of new certificate issuance to subscriber
4.7.5 Conduct constituting acceptance of a re-keyed certificate
4.7.6 Publication of the re-keyed certificate by the CA
4.7.7 Notification of certificate issuance by the CA to other entities
4.8 Certificate modification
4.8.1 Circumstance for certificate modification
4.8.2 Who may request certificate modification
4.8.3 Processing certificate modification requests
4.8.4 Notification of new certificate issuance to subscriber
4.8.5 Conduct constituting acceptance of modified certificate
4.8.6 Publication of the modified certificate by the CA
4.8.7 Notification of certificate issuance by the CA to other entities
4.9 Certificate revocation and suspension
4.9.1 Circumstances for revocation
4.9.1.1 Reasons for Revoking a Subscriber Certificate
4.9.1.2 Reasons for Revoking a Subordinate CA Certificate
4.9.2 Who can request revocation
4.9.3 Procedure for revocation request
4.9.4 Revocation request grace period

4.9.5 Time within which CA must process the revocation request
4.9.6 Revocation checking requirement for relying parties
4.9.7 CRL issuance frequency (if applicable)
4.9.7.1 For the status of Subscriber Certificates
4.9.7.2 For the status of Subordinate CA Certificates
4.9.8 Maximum latency for CRLs (if applicable)
4.9.9 On-line revocation/status checking availability
4.9.10 On-line revocation checking requirements
4.9.10.1 For the status of Subscriber Certificates
4.9.10.2 For the status of Subordinate CA Certificates
4.9.11 Other forms of revocation advertisements available
4.9.12 Special requirements re key compromise
4.9.13 Circumstances for suspension
4.9.14 Who can request suspension
4.9.15 Procedure for suspension request
4.9.16 Limits on suspension period
4.10 Certificate status services
4.10.1 Operational characteristics
4.10.2 Service availability
4.10.3 Optional features
4.11 End of subscription
4.12 Key escrow and recovery
4.12.1 Key escrow and recovery policy and practices
4.12.2 Session key encapsulation and recovery policy and practices
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS
5.1 Physical controls
5.1.1 Site location and construction
5.1.2 Physical access
5.1.3 Power and air conditioning
5.1.4 Water exposures
5.1.5 Fire prevention and protection
5.1.6 Media storage
5.1.7 Waste disposal
5.1.8 Off-site backup
5.2 Procedural controls
5.2.1 Trusted roles
5.2.2 Number of persons required per task
5.2.3 Identification and authentication for each role
5.2.4 Roles requiring separation of duties
5.3 Personnel controls
5.3.1 Qualifications, experience, and clearance requirements
5.3.2 Background check procedures
5.3.3 Training requirements
5.3.4 Retraining frequency and requirements
5.3.5 Job rotation frequency and sequence
5.3.6 Sanctions for unauthorized actions
5.3.7 Independent contractor requirements

5.3.8 Documentation supplied to personnel
5.4 Audit logging procedures
5.4.1 Types of events recorded
5.4.2 Frequency of processing log
5.4.3 Retention period for audit log
5.4.4 Protection of audit log
5.4.5 Audit log backup procedures
5.4.6 Audit collection system (internal vs. external)
5.4.7 Notification to event-causing subject
5.4.8 Vulnerability assessments
5.5 Records archival
5.5.1 Types of records archived
5.5.2 Retention period for archive
5.5.3 Protection of archive
5.5.4 Archive backup procedures
5.5.5 Requirements for time-stamping of records
5.5.6 Archive collection system (internal or external)
5.5.7 Procedures to obtain and verify archive information
5.6 Key changeover
5.7 Compromise and disaster recovery
5.7.1 Incident and compromise handling procedures
5.7.2 Computing resources, software, and/or data are corrupted
5.7.3 Entity private key compromise procedures
5.7.4 Business continuity capabilities after a disaster
5.8 CA or RA termination
6 TECHNICAL SECURITY CONTROLS
6.1 Key pair generation and installation
6.1.1 Key pair generation
6.1.1.1 CA Key Pair Generation
6.1.1.2 RA Key Pair Generation
6.1.1.3 Subscriber Key Pair Generation
6.1.2 Private key delivery to subscriber
6.1.3 Public key delivery to certificate issuer
6.1.4 CA public key delivery to relying parties
6.1.5 Key sizes
6.1.5.1 Root CA Certificates
6.1.5.2 Subordinate CA Certificates
6.1.5.3 Subscriber Certificates
6.1.6 Public key parameters generation and quality checking
6.1.7 Key usage purposes (as per X.509 v3 key usage field)
6.2 Private Key Protection and Cryptographic Module Engineering Controls
6.2.1 Cryptographic module standards and controls
6.2.2 Private key (n out of m) multi-person control
6.2.3 Private key escrow
6.2.4 Private key backup
6.2.5 Private key archival
6.2.6 Private key transfer into or from a cryptographic module

6.2.7 Private key storage on cryptographic module
6.2.8 Method of activating private key
6.2.9 Method of deactivating private key
6.2.10 Method of destroying private key
6.2.11 Cryptographic Module Rating
6.3 Other aspects of key pair management
6.3.1 Public key archival
6.3.2 Certificate operational periods and key pair usage periods
6.4 Activation data
6.4.1 Activation data generation and installation
6.4.2 Activation data protection
6.4.3 Other aspects of activation data
6.5 Computer security controls
6.5.1 Specific computer security technical requirements
6.5.1.1 Account Management
6.5.1.2 Least Privilege
6.5.1.3 Access Control Best Practices
6.5.1.4 Authentication: Passwords and Accounts
6.5.1.5 System Isolation and Partitioning
6.5.1.6 Malicious Code Protection
6.5.1.7 Software and Firmware Integrity
6.5.2 Computer security rating
6.6 Life cycle technical controls
6.6.1 System development controls
6.6.2 Security management controls
6.6.3 Life cycle security controls
6.7 Network security controls
6.7.1 Boundary Systems
6.7.1.1 PKI Network Zones Overview
6.7.1.2 Special Access Zone Boundary
6.7.1.3 Restricted Zone Boundary
6.7.1.4 Operational Zone Boundary
6.7.2 Network Monitoring
6.7.2.1 Monitoring devices
6.7.2.2 Monitoring of Security Alerts, Advisories, and Directives
6.7.3 Remote Access/External Information Systems
6.7.4 Penetration Testing
6.8 Time-stamping
7 CERTIFICATE, CRL, AND OCSP PROFILES
7.1 Certificate profile
7.1.1 Version number(s)
7.1.2 Certificate extensions
7.1.2.1 Root CA Certificate
7.1.2.2 Subordinate CA Certificate
7.1.2.3 Subscriber Certificate
7.1.2.4 All Certificates
7.1.2.5 Application of RFC 5280

7.1.3 Algorithm object identifiers
7.1.4 Name forms
7.1.4.1 Issuing CA Certificate Subject
7.1.4.2 Subject Information for Standard Server Authentication certificates
7.1.4.3 Subject Alternative Names for Standard Server Authentication certificates
7.1.4.4 Subject Information for Extended Validation Server Authentication certificates
7.1.4.5 Subject Alternative Names for Extended Validation Server Authentication certificates
7.1.4.6 Subject Information for Extended Validation Code Signing certificates
7.1.5 Name constraints
7.1.6 Certificate policy object identifier
7.1.6.1. Reserved Certificate Policy Identifiers
7.1.6.2. Root CA Certificates
7.1.6.3 Subordinate CA Certificates
7.1.6.4 Subscriber Certificates
7.1.7 Usage of Policy Constraints extension
7.1.8 Policy qualifiers syntax and semantics
7.1.9 Processing semantics for the critical Certificate Policies extension
7.2 CRL profile
7.2.1 Version number(s)
7.2.2 CRL and CRL entry extensions
7.3 OCSP profile
7.3.1 Version number(s)
7.3.2 OCSP extensions
8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS
8.1 Frequency or circumstances of assessment
8.2 Identity/qualifications of assessor
8.3 Assessor's relationship to assessed entity
8.4 Topics covered by assessment
8.5 Actions taken as a result of deficiency
8.6 Communication of results
8.7 Self-Audits
9 OTHER BUSINESS AND LEGAL MATTERS
9.1 Fees
9.1.1 Certificate issuance or renewal fees
9.1.2 Certificate access fees
9.1.3 Revocation or status information access fees
9.1.4 Fees for other services
9.1.5 Refund policy
9.2 Financial responsibility
9.2.1 Insurance coverage
9.2.2 Other assets
9.2.3 Insurance or warranty coverage for end-entities
9.3 Confidentiality of business information
9.3.1 Scope of confidential information
9.3.2 Information not within the scope of confidential information
9.3.3 Responsibility to protect confidential information

9.4 Privacy of personal information
9.4.1 Privacy plan
9.4.2 Information treated as private
9.4.3 Information not deemed private
9.4.4 Responsibility to protect private information
9.4.5 Notice and consent to use private information
9.4.6 Disclosure pursuant to judicial or administrative process
9.4.7 Other information disclosure circumstances
9.5 Intellectual property rights
9.6 Representations and warranties
9.6.1 CA representations and warranties
9.6.2 RA representations and warranties
9.6.3 Subscriber representations and warranties
9.6.4 Relying party representations and warranties
9.6.5 Representations and warranties of other participants
9.7 Disclaimers of warranties
9.8 Limitations of liability
9.9 Indemnities
9.10 Term and termination
9.10.1 Term
9.10.2 Termination
9.10.3 Effect of termination and survival
9.11 Individual notices and communications with participants
9.12 Amendments
9.12.1 Procedure for amendment
9.12.2 Notification mechanism and period
9.12.3 Circumstances under which OID must be changed
9.13 Dispute resolution provisions
9.14 Governing law
9.15 Compliance with applicable law
9.16 Miscellaneous provisions
9.16.1 Entire agreement
9.16.2 Assignment
9.16.3 Severability
9.16.4 Enforcement (attorneys' fees and waiver of rights)
9.16.5 Force Majeure
9.17 Other provisions

1 INTRODUCTION

1.1 Overview

This Certificate Policy is intended to communicate the minimum operating requirements for CAs in the Amazon PKI. By design, it closely follows the CA/Browser Forum Guidelines and Requirements and only deviates when an Application Software Supplier has requirements that are stricter than those published by the CA/Browser Forum.

This CP also includes the principles and criteria that CAs are required to follow according to the Trust Service Principles and Criteria for Certification Authorities Version 2.0.

This CP does not attempt to paraphrase or alter the requirements, rather the focus is to bring all of them into one document to enable Relying Parties and auditors to have a comprehensive view of the policies which the CA commits to follow.

Certificate Authorities following this CP may have practices which exceed the minimum requirements set forth by these policies. CAs may also describe practices that cover topics for which there is no stipulation in this CP.

1.1.1 Compliance

This Certificate Policy conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org (http://www.cabforum.org). In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

This Certificate Policy conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

This CP conforms to the current version of the CA/Browser Forum Guidelines for Issuance and Management of Extended Validation Code Signing Certificates published at http://www.cabforum.org. In the event of any inconsistency between this document and those Guidelines, those Guidelines take precedence over this document.

1.1.2 Types of Certificates

This Certificate Policy defines several different types of certificates. Each certificate issued under this policy is categorized as either a CA-certificate or an End-Entity Certificate.

All certificates issued under this policy MUST be X.509 v3 certificates.

1.1.2.1 CA-Certificates

A certificate is a CA-certificate if basicConstraints extension is present and has cA:TRUE.

CA-certificates are grouped into two categories: self-issued certificates and cross-certificates.

A self-issued certificate is a CA certificate where the subject and issuer DNs of the certificate match. Under this policy, all self-issued certificates must be self-signed certificates. A self-signed certificate is a self-issued certificate where the private key used by the CA to sign the certificate corresponds to the public key that is certified within the certificate.

A cross-certificate is a CA certificate that is not a self-issued certificate.

1.1.2.1.3 Terminus CA-Certificates

A certificate is a Terminus CA-certificate if it is a cross-certificate and the basicConstraints extension is present and the pathLenConstraint is present and set to 0 (zero).

1.1.2.1.4 Policy CA-Certificates

A certificate is a Policy CA-certificate if it is a cross-certificate and is not a Terminus CA-certificate.

1.1.2.1.5 Technically Constrained CA-Certificates

A certificate is a Technically Constrained CA-certificate if it is a CA-certificate and it meets the requirements in section 7.1.5.

1.1.2.1.6 Unconstrained CA-Certificates

A certificate is an Unconstrained CA-certificate if it is a CA-certificate and is not a Technically Constrained CA-certificate.

1.1.2.1.7 Root CA-Certificates

A certificate is a Root CA-certificate if the subject is designated by the CA as a Root CA in the CA's CPS and it is either a self-issued certificate or Policy CA-certificate.

1.1.2.1.8 Subordinate CA-Certificates

A certificate is a Subordinate CA-certificate if it is a cross-certificate and the subject DN of the certificate does not match the issuer name of any Root CA in the CA's CPS.

1.1.2.2 End-Entity Certificates

A certificate is an End-Entity Certificate if it is not a CA certificate.

End-Entity Certificates can be further broken down into the following categories. CAs must not issue End-Entity Certificates that simultaneously meet the criteria of multiple of the following categories.

1.1.2.2.1 Extended Validation TLS Server Authentication Certificates

An End-Entity Certificate is an Extended Validation TLS Server Authentication Certificate if it (i) has a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-serverAuth (1.3.6.1.5.5.7.3.1) in the Extended Key Usage certificate extension.

1.1.2.2.2 Standard Validation TLS Server Authentication Certificates

An End-Entity Certificate is a Standard Validation TLS Server Authentication Certificate if it (i) does not have a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-serverAuth (1.3.6.1.5.5.7.3.1) in the Extended Key Usage certificate extension.

1.1.2.2.3 Extended Validation Code Signing Certificates

An End-Entity Certificate is an Extended Validation Code Signing Certificate if it (i) has a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-codeSigning (1.3.6.1.5.5.7.3.3) in the Extended Key Usage certificate extension.

1.1.2.2.4 Standard Validation Code Signing Certificates

An End-Entity Certificate is a Standard Validation Code Signing Certificate if it (i) does not have a Relative Distinguished Name of type jurisdictionOfIncorporationCountryName (1.3.6.1.4.1.311.60.2.1.3) in the Subject Distinguished Name and (ii) has a key purpose of id-kp-codeSigning (1.3.6.1.5.5.7.3.3) in the Extended Key Usage certificate extension.

1.1.2.2.5 Client Certificates (including Augmented Client Certificates)

An End-Entity Certificate is a Client Certificate if it has at least one of id-kp-clientAuth (1.3.6.1.5.5.7.3.2), id-kp-emailProtection (1.3.6.1.5.5.7.3.4), Document Signing (1.3.6.1.4.1.311.10.3.12), or Encrypting Filesystem Crypto (1.3.6.1.4.1.311.10.3.4) key purposes in the Extended Key Usage certificate extension and does not have the id-kp-serverAuth (1.3.6.1.5.5.7.3.1) key purpose in the Extended Key Usage certificate extension.

Under this policy, an Augmented Client Certificate is identical to a Client Certificate.

1.1.2.2.6 OCSP Signing Certificate

An End-Entity Certificate is an OCSP Signing Certificate if it has a key purpose of id-kp-OCSPSigning (1.3.6.1.5.5.7.3.9) in the Extended Key Usage certificate extension.

1.1.2.2.7 Time Stamp Authority Certificate

An End-Entity Certificate is a Time Stamping Authority Certificate if it has a key purpose of id-kp-timeStamping (1.3.6.1.5.5.7.3.8) in the Extended Key Usage certificate extension.

1.1.2.3 Subscriber Certificates

All Extended Validation TLS Server Authentication Certificates, Standard Validation TLS Server Authentication Certificates, and Extended Validation Code Signing Certificates are Subscriber Certificates.

1.2 Document name and identification

This is the Amazon Public Key Infrastructure (PKI) Certificate Policy. It was approved for publication by the Amazon PKI Policy Management Authority (APPMA). Amendments are made only after the APPMA has reviewed and approved such amendment. This document is identified by the Object Identifier 1.3.187.16385.1.

This CP is updated at least annually to ensure that it incorporates the latest version of the CA/Browser Forum Baseline Requirements.

Date	Changes	Version
2017-01-12	Yearly update	1.0.4
2018-01-15	Yearly update	1.0.5
2018-04-13	Updated 3.2.2.4 Validation of Domain Authorization or Control, BR 1.5.6	1.0.6

1.3 PKI participants

1.3.1 Certification authorities

The Certification Authority (CA) provides services in accordance with its disclosed practices.

1.3.2 Registration authorities

The CA MAY delegate the performance of all, or any part, of Section 3.2 requirements to a Delegated Third Party, provided that the process as a whole fulfills all of the requirements of Section 3.2.

Before the CA authorizes a Delegated Third Party to perform a delegated function, the CA SHALL contractually require the Delegated Third Party to:

1. Meet the qualification requirements of Section 5.3.1, when applicable to the delegated function;
2. Retain documentation in accordance with Section 5.5.2;
3. Abide by the other provisions of these Requirements that are applicable to the delegated function; and
4. Comply with (a) the CA's Certificate Policy/Certification Practice Statement or (b) the Delegated Third Party's practice statement that the CA has verified complies with these Requirements.

The CA MAY designate an Enterprise RA to verify certificate requests from the Enterprise RA's own organization. The CA SHALL NOT accept certificate requests authorized by an Enterprise RA unless the following requirements are satisfied:

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

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

The CA MAY contractually authorize the Subject of a specified Valid EV Certificate to perform the RA function and authorize the CA to issue Enterprise EV Certificates. In such case, the Subject SHALL be considered an Enterprise RA, and the following requirements SHALL apply:

1. An Enterprise RA SHALL NOT authorize the CA to issue an Enterprise EV Certificate at the third or higher domain levels to any Subject other than the Enterprise RA or a business that is owned or directly controlled by the Enterprise RA;
2. In all cases, the Subject of an Enterprise EV Certificate MUST be an organization verified by the CA in accordance with this Certificate Policy;
3. The CA MUST impose these limitations as a contractual requirement with the Enterprise RA and monitor compliance by the Enterprise RA;
4. The Final Cross-Correlation and Due Diligence requirements of EV Guidelines Section 11.13 MAY be performed by a single person representing the Enterprise RA; and
5. The audit requirements of EV Guidelines Section 17.1 SHALL apply to the Enterprise RA, except in the case where the CA maintains control over the Root CA Private Key or Subordinate CA Private Key used to issue the Enterprise EV Certificates, in which case, the Enterprise RA MAY be exempted from the audit requirements.

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

1.3.3 Subscribers

No stipulation.

1.3.4 Relying parties

No stipulation.

1.3.5 Other participants

The CA MUST include (directly or by reference) the applicable requirements of the EV Guidelines in all contracts with Subordinate CAs, RAs, Enterprise RAs, and subcontractors that involve or relate to the issuance or maintenance of EV Certificates. The CA MUST enforce compliance with such terms.

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

The CA MUST include (directly or by reference) the applicable requirements of this Certificate Policy in all contracts that involve or relate to the issuance or maintenance of EV Code Signing Certificates. The Issuer MUST enforce compliance with such terms.

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

1.4 Certificate usage

1.4.1 Appropriate certificate uses

No stipulation.

1.4.2 Prohibited certificate uses

No stipulation.

1.5 Policy administration

The CA must disclose its business practices including but not limited to the topics listed in RFC 3647, RFC 2527, or WebTrust for Certification Authorities v1 CA Business Practices Disclosure Criteria in its Certification Practice Statement.

The CA must maintain controls to provide reasonable assurance that its Certification Practice Statement management processes are effective.

Each CA MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Certificate practices, policies and procedures that:

1. Implements this policy;
2. Implements the requirements of (i) the then-current WebTrust Program for CAs, and (ii) the then-current WebTrust EV Program or ETSI TS 102 042; and
3. Specifies the CA's and its Root CA's entire root certificate hierarchy including all roots that its EV Certificates depend on for proof of those EV Certificates' authenticity.

Each Issuer MUST develop, implement, enforce, display prominently on its Web site, and periodically update as necessary its own auditable EV Code Signing Object practices, policies and procedures, such as a Certification Practice Statement and Certificate Policy that:

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

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

Ordinarily, a code signature created by a Subscriber may be considered valid for a period of up to thirty-nine months. However, a code signature may be treated as valid for a period of up to one hundred and twenty three months by means of one of the following methods: the "Timestamp" Method or the "Signing Authority" Method.

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

1.5.1 Organization administering the document

No stipulation.

1.5.2 Contact person

No stipulation.

1.5.3 Person determining CPS suitability for the policy

The CA must maintain controls to provide reasonable assurance that its Certification Practice Statement addresses the topics included in its Certificate Policy.

1.5.4 CPS approval procedures

No stipulation.

1.6 Definitions and acronyms

1.6.1 Definitions

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.

Affiliate
: A 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.

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 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 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 the Baseline Requirements.

Baseline Requirements
: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.

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.

CAA Record

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 Records allows a public Certification Authority to implement additional controls to reduce the risk of unintended certificate mis-issue."

Certificate

An electronic document that uses a digital signature to bind a public key and an identity.

Certificate Approver

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

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 the CA has access.

Certificate Management Process

Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.

Certificate Management System

A system used by a CA or Delegated Third Party to process, approve issuance of, or store certificates or certificate status information, including the database, database server, and storage.

Certificate Policy

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

A regularly updated time-stamped list of revoked Certificates that is created and digitally signed by the CA that issued the Certificates.

Certificate Systems

The system used by a CA or Delegated Third Party in providing identity verification, registration and enrollment, certificate approval, issuance, validity status, support, and other PKI-related services.

Certification Authority

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 Practice Statement

One of several documents forming the governance framework in which Certificates are created, issued, managed, and used.

Common Vulnerability Scoring System (CVSS)

A quantitative model used to measure the base level severity of a vulnerability (see http://nvd.nist.gov/home.cfm).

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%.

Country

Either a member of the United Nations OR a geographic region recognized as a sovereign nation by at least two UN member nations.

Critical Security Event

Detection of an event, a set of circumstances, or anomalous activity that could lead to a circumvention of a Zone's security controls or a compromise of a Certificate System's integrity, including excessive login attempts, attempts to access prohibited resources, DoS/DDoS attacks, attacker reconnaissance, excessive traffic at unusual hours, signs of unauthorized access, system intrusion, or an actual compromise of component integrity.

Critical Vulnerability

A system vulnerability that has a CVSS score of 7.0 or higher according to the NVD or an equivalent to such CVSS rating (see http://nvd.nist.gov/home.cfm), or as otherwise designated as a Critical Vulnerability by the CA or the CA/Browser Forum.

Cross Certificate

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

Delegated Third Party

A natural person or Legal Entity that is not the CA 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.

Delegated Third Party System

Any part of a Certificate System used by a Delegated Third Party while performing the functions delegated to it by the CA.

Demand Deposit Account

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

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 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 the CA who authorizes issuance of Certificates to that organization.

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 the EV Guidelines.

EV Certificate

A certificate that contains subject information specified in the EV Guidelines and that has been validated in accordance with the EV 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 the EV 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 this Certificate Policy and that has been validated in accordance with this Certificate Policy.

EV Code Signing Object

An EV Code Signing Certificate issued by a CA or an EV Signature provided by a Signing Authority.

EV Guidelines

Guidelines For The Issuance And Management Of Extended Validation Certificates published by the CA/Browser Forum

EV OID

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

Expiry Date

The "Not After" date in a Certificate that defines the end of a Certificate's validity period.

Extended Validation Certificate

See EV Certificate.

Front End / Internal Support System

A system with a public IP address, including a web server, mail server, DNS server, jump host, or authentication server.

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 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, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Government Entity

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, county, etc.).

High Risk Certificate Request

A Request that the CA 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, names listed on the Miller Smiles phishing list or the Google Safe Browsing list, or names that the CA identifies using its own risk-mitigation criteria.

High Security Zone

A physical location where a CA's or Delegated Third Party's Private Key or cryptographic hardware is located.

Incorporating Agency

In the context of a Private Organization, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Government Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Government Entities.

Independent Confirmation From Applicant

Confirmation of a particular fact received by the CA pursuant to the provisions of the EV Guidelines or binding upon the Applicant.

Individual

A natural person.

Internal Name

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

International Organization

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

Issuer

A CA providing an EV Code Signing Certificate to a Subscriber or a Signing Authority that provides an EV signature for a Subscriber.

Issuing CA

In relation to a particular Certificate, the CA that issued the Certificate. This could be either a Root CA or a Subordinate CA.

Issuing System

A system used to sign certificates or validity status information.

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 Script

A documented plan of procedures for the generation of a CA Key Pair.

Key Pair

The Private Key and its associated Public Key.

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 the EV Guidelines and competent to render an opinion on factual claims of the Applicant.

Maximum Validity Period

1. The maximum time period for which the issued EV Certificate is valid. 2. The maximum period after validation by the CA that certain Applicant information may be relied upon in issuing an EV Certificate pursuant to the EV Guidelines.

National Vulnerability Database (NVD)

A database that includes the Common Vulnerability Scoring System (CVSS) scores of security-related software flaws, misconfigurations, and vulnerabilities associated with systems (see http://nvd.nist.gov/home.cfm).

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 Responder

An online server operated under the authority of the CA and connected to its Repository for processing Certificate status requests. See also, Online Certificate Status Protocol.

Online Certificate Status Protocol

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

OWASP Top Ten

A list of application vulnerabilities published by the Open Web Application Security Project (see https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project).

Parent CA

The CA which issues a Subordinate CA Certificate

Parent Company

A company that Controls a Subsidiary Company.

Penetration Test

A process that identifies and attempts to exploit openings and vulnerabilities on systems through the active use of known attack techniques, including the combination of different types of exploits, with a goal of breaking through layers of defenses and reporting on unpatched vulnerabilities and system weaknesses.

Place of Business

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

Principal Individual

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

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

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.

Qualified Auditor

A natural person or Legal Entity that meets the requirements of Section 8.2.

Qualified Government Information Source

A database maintained by a Government Entity (e.g. SEC filings) that meets the requirements of Section 11.11.6 of the EV Guidelines.

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.

Registered Agent

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

Registered Domain Name

A Domain Name that has been registered with a Domain Name Registrar.

Registered Office

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

Registration Agency

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

Registration Authority (RA)

Any 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.

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.

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/ipv4-address-space/ipv4-address-space.xml) http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml (http://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xml)

Root CA

The top level Certification Authority whose Root Certificate is distributed by Application Software Suppliers and that issues Subordinate CA Certificates.

Root CA System

A system used to create a Root Certificate or to generate, store, or sign with the Private Key associated with a Root Certificate.

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 Key Generation Script

A documented plan of procedures to be performed for the generation of the Root CA Key Pair.

SANS Top 25

A list created with input from the SANS Institute and the Common Weakness Enumeration (CWE) that identifies the Top 25 Most Dangerous Software Errors that lead to exploitable vulnerabilities (see http://www.sans.org/top25-software-errors/).

Secure Zone

An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of Certificate Systems.

Security Support System

A system used to provide security support functions, such as authentication, network boundary control, audit logging, audit log reduction and analysis, vulnerability scanning, and antivirus.

Signing Authority

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

Sovereign State

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

Subject

The natural person, device, system, unit, or Legal Entity identified in a Certificate as the Subject. The Subject is either the Subscriber or a device under the control and operation of the Subscriber.

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

A natural person or Legal Entity to whom a Certificate is issued and who is legally bound by a Subscriber or Terms of Use Agreement.

Subscriber Agreement

An agreement between the CA and the Applicant/Subscriber that specifies the rights and responsibilities of the parties.

Subsidiary Company

A company that is controlled by a Parent Company.

Superior Government Entity

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

Suspect code

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

System

One or more pieces of equipment or software that stores, transforms, or communicates data.

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 this CP when the Applicant/Subscriber is an Affiliate of the CA.

Timestamp Authority

An organization that timestamps data, thereby asserting that the data existed at the specified time;

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 Role

An employee or contractor of a CA or Delegated Third Party who has authorized access to or control over a Secure Zone or High Security Zone.

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.

Unregistered Domain Name

A Domain Name that is not a Registered Domain Name.

Valid Certificate

A Certificate that passes the validation procedure specified in RFC 5280.

Validation Specialists

Someone who performs the information verification duties specified by this CP.

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 the EV Guidelines

Verified Legal Opinion

A document meeting the requirements specified in Section 11.11.1 of the EV 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 EV Guidelines as a reliable way of communicating with the Applicant.

Vulnerability Scan

A process that uses manual or automated tools to probe internal and external systems to check and report on the status of operating systems, services, and devices exposed to the network and the presence of vulnerabilities listed in the NVD, OWASP Top Ten, or SANS Top 25.

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.

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.

Zone
: A subset of Certificate Systems created by the logical or physical partitioning of systems from other Certificate Systems.

1.6.2 Acronyms

ADF
: Application Data File

AICPA
: American Institute of Certified Public Accountants

BIPM
: International Bureau of Weights and Measures

BIS
: (US Government) Bureau of Industry and Security

CA
: Certification Authority

CAA
: Certification Authority Authorization

ccTLD
: Country Code Top-Level Domain

CEO
: Chief Executive Officer

CFO
: Chief Financial Officer

CICA
: Canadian Institute of Chartered Accountants

CIO
: Chief Information Officer

CISO
: Chief Information Security Officer

COO
: Chief Operating Officer

CP
: Certificate Policy

CPA
: Chartered Professional Accountant

CPS
: Certification Practice Statement

CRL
: Certificate Revocation List

CSO
: Chief Security Officer

DBA
: Doing Business As

DNS
: Domain Name System

ETSI
: European Telecommunications Standards Institute

EV
: Extended Validation

FIPS
: (US Government) Federal Information Processing Standard

FQDN
: Fully Qualified Domain Name

gTLD
: Generic Top-Level Domain

IANA
: Internet Assigned Numbers Authority

ICANN
: Internet Corporation for Assigned Names and Numbers

ICC
: Integrated Circuit Card

IFAC
: International Federation of Accountants

IM
: Instant Messaging

IRS
: Internal Revenue Service

ISO
: International Organization for Standardization

ISP
: Internet Service Provider

NIST
: (US Government) National Institute of Standards and Technology

OCSP
: Online Certificate Status Protocol

OID
: Object Identifier

PKI
: Public Key Infrastructure

QGIS

Qualified Government Information Source

QIIS

Qualified Independent Information Source

QTIS

Qualified Government Tax Information Source

RA

Registration Authority

S/MIME

Secure MIME (Multipurpose Internet Mail Extensions)

SEC

(US Government) Securities and Exchange Commission

SSL

Secure Sockets Layer

TLD

Top-Level Domain

TLS

Transport Layer Security

UTC(k)

National realization of Coordinated Universal Time

VOIP

Voice Over Internet Protocol

1.6.3 References

ETSI TS 119 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - General Requirements and Guidance.

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.

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.

RFC2560, Request for Comments: 2560, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP M. Myers, et al, June 1999.

RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

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.

WebTrust for Certification Authorities, SSL Baseline with Network Security, Version 2.0, available at http://www.webtrust.org/homepage-documents/item79806.pdf.

X.509v3 , ITU-T Recommendation X.509 (2005) | ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

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

The CA SHALL develop, implement, enforce, and annually update a Certification Practice Statement that describes in detail how the CA implements the latest version of these Requirements.

2.1 Repositories

The CA SHALL make revocation information for Subordinate Certificates and Subscriber Certificates available in accordance with this Policy.

2.2 Publication of certification information

The Parent CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including CRLs and other certificate status mechanisms) is made available to any entity in accordance with the CA’s disclosed business practices.

The CA SHALL publicly disclose its Certificate Policy and/or Certification Practice Statement through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA business practices to the extent required by the CA’s selected audit scheme (see Section 8.1). The disclosures MUST include all the material required by RFC 2527 or RFC 3647, and MUST be structured in accordance with either RFC 2527 or RFC 3647. Effective as of 15 April 2015, section 4.2 of a CA’s Certificate Policy and/or Certification Practice Statement (section 4.1 for CAs still conforming to RFC 2527) SHALL state whether the CA reviews CAA Records, and if so, the CA’s policy or practice on processing CAA Records for Fully Qualified Domain Names. The CA SHALL log all actions taken, if any, consistent with its processing practice.

The CA SHALL host test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates that chain up to each publicly trusted Root Certificate. At a minimum, the CA SHALL host separate Web pages using Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

The CA MUST host test Web pages that allow Application Software Suppliers to test their software with EV Certificates that chain up to each EV Root Certificate. At a minimum, the CA MUST host separate Web pages using certificates that are (i) valid (ii) revoked and (iii) expired.

Each CA MUST publicly disclose their EV Policies through an appropriate and readily accessible online means that is available on a 24x7 basis. The CA is also REQUIRED to publicly disclose its CA business practices as required by both WebTrust for CAs and ETSI TS 102 042. The disclosures MUST be structured in accordance with either RFC 2527 or RFC 3647.

2.3 Time or frequency of publication

No stipulation.

2.4 Access controls on repositories

No stipulation.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

No stipulation.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

3.2 Initial identity validation

The Certification Authority maintains controls to provide reasonable assurance that Subscriber information was properly authenticated (for the registration activities performed by the CA).

The CA maintains controls to provide reasonable assurance that, for authenticated Certificates, Subscribers are accurately identified in accordance with the CA's disclosed business practices.

For EV Certificates, in cases where the Certificate Request does not contain all necessary information about the Applicant, the CA MUST additionally confirm the data with the Certificate Approver or Contract Signer rather than the Certificate Requester.

Before issuing an EV Certificate, the CA MUST ensure that all Subject organization information to be included in the EV Certificate conforms to the requirements of, and is verified in accordance with, this Certificate Policy and matches the information confirmed and documented by the CA pursuant to its verification processes. Such verification processes are intended to accomplish the following:

1. Verify Applicant's existence and identity, including:

    A. Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 of the EV Guidelines),
    B. Verify the Applicant's physical existence (business presence at a physical address), and 3.Verify the Applicant's operational existence (business activity).
2. Verify the Applicant is a registered holder, or has control, of the Domain Name(s) to be included in the EV Certificate;
3. Verify a reliable means of communication with the entity to be named as the Subject in the Certificate;
4. Verify the Applicant's authorization for the EV Certificate, including;

    A. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    B. Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    C. Verify that a Certificate Approver has signed or otherwise approved the EV Certificate Request.

As a general rule, the CA is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth in Sections 11.2 through 11.14 of the EV Guidelines. The Acceptable Methods of Verification set forth in each of Sections 11.2 through 11.14 of the EV Guidelines are considered to be the minimum acceptable level of verification required of the CA. In all cases, however, the CA is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

Before issuing an EV Code Signing Object, the Issuer MUST ensure that all Subject organization information to be included in the EV Code Signing Object conforms to the requirements of, and is verified in accordance with the EV Guidelines and matches the information confirmed and documented by the Issuer pursuant to its verification processes. Such verification processes are intended to accomplish the following:

1. Verify Applicant's existence and identity, including;

    A. Verify the Applicant's legal existence and identity (as more fully set forth in Section 11.2 of the EV Code Signing Guidelines),
    B. Verify the Applicant's physical existence (business presence at a physical address), and
    C. Verify the Applicant's operational existence (business activity).

2. Verify the Applicant's authorization for the EV Code Signing Certificate, including;

    A. Verify the name, title, and authority of the Contract Signer, Certificate Approver, and Certificate Requester,
    B. Verify that a Contract Signer signed the Subscriber Agreement or that a duly authorized Applicant Representative acknowledged and agreed to the Terms of Use; and
    C. Verify that a Certificate Approver has signed or otherwise approved the EV Code Signing Certificate Request.

An EV Timestamp Authority is NOT REQUIRED to validate in any way data submitted to it for time-stamping. It simply adds the time to the data that are presented to it, signs the result and appends its own certificate.

As a general rule, the Issuer of EV Code Signing Certificates is responsible for taking all verification steps reasonably necessary to satisfy each of the Verification Requirements set forth Sections 11.2 through 11.14 of the EV Code Signing Guidelines. The Acceptable Methods of Verification are set forth in the EV Guidelines. In all cases, however, the Issuer is responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

3.2.1 Method to prove possession of private key

No stipulation.

3.2.2 Validation of Domain Authorization or Control

If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA 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 the CA's Certificate Policy and/or Certification Practice Statement. If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA 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 the CA's Certificate Policy and/or Certification Practice Statement. The CA SHALL inspect any document relied upon under this Section for alteration or falsification.

If the Applicant requests an Extended Validation Certificate, then the CA shall follow the EV Guidelines.

3.2.2.1 Identity

If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:

1. A Government Agency in the Applicant's Jurisdiction of Incorporation or Jurisdiction of Registration;
2. A third party database that is periodically updated and considered a Reliable Data Source;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation Letter.

The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

Alternatively, the CA 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 the CA determines to be reliable.

3.2.2.2 DBA/Tradename

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

3.2.2.3 Verification of Country

If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following: (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; (c) information provided by the Domain Name Registrar; or (d) a method identified in Section 3.2.2.1. The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.

3.2.2.4 Validation of Domain Authorization or Control

The CA maintains controls to provide reasonable assurance that, for domain validated certificates, subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices.

The CA maintains controls to provide reasonable assurance that, for domain validated certificates, subscribers' domain names are accurately validated in accordance with the CA's disclosed business practices.

The CA SHALL confirm that prior to issuance, the CA 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.

CAs SHALL maintain a record of which domain validation method, including relevant BR version number, they used to validate every domain.

3.2.2.4.1 Validating the Applicant as a Domain Contact

Amazon does not use this retired method.

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.

The CA 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.

The CA 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 the CA MUST follow its CPS.

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. The CA 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.

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.

3.2.2.4.5 Domain Authorization Document

Amazon does not use this retired method.

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 the CA 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
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, the CA 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.

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, the CA 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.

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.

3.2.2.4.9 Test Certificate

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

3.2.2.4.10. TLS Using a Random Number

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

3.2.2.4.11 Any Other Method

Amazon does not use this retired method.

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 the CA is also the Domain Name Registrar, or an Affiliate of the Registrar, of the Base Domain Name.

3.2.2.5 Authentication for an IP Address

For each IP Address listed in a Certificate, the CA 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 the CA 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, the CA MUST establish and follow a documented procedure[1] that determines if the wildcard character occurs in the first label position to the left of a "registry-controlled" label or "public suffix" (e.g. "*.com", "*.co.uk", see RFC 6454 Section 8.2 for further explanation).

If a wildcard would fall within the label immediately to the left of a registry-controlled[1] or public suffix, CAs MUST refuse issuance unless the applicant proves its rightful control of the entire Domain Namespace. (e.g. CAs 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, the CA SHALL evaluate the source for its reliability, accuracy, and resistance to alteration or falsification. The CA 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 the CA, 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 Section 3.2.

3.2.3 Authentication of individual identity

If an Applicant subject to this Section is an Individual, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request.

The CA SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification.

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

The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.

If the Applicant requests an Extended Validation Certificate, then the CA shall follow the EV Guidelines.

3.2.4 Non-verified subscriber information

No stipulation.

3.2.5 Validation of authority

The CA maintains controls to provide reasonable assurance that, for authenticated certificates, Subscriber's certificate requests are accurate, authorized and complete.

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

The CA MAY use the sources listed in section 3.2.2.1 to verify the Reliable Method of Communication. Provided that the CA uses a Reliable Method of Communication, the CA 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 the CA deems appropriate.

In addition, the CA SHALL establish a process that allows an Applicant to specify the individuals who may request Certificates. If an Applicant specifies, in writing, the individuals who may request a Certificate, then the CA SHALL NOT accept any certificate requests that are outside this specification. The CA 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

The CA SHALL disclose all Cross Certificates that identify the CA as the Subject, provided that the CA 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

3.3.1 Identification and authentication for routine re-key

Section 6.3.2 limits the validity period of Subscriber Certificates. The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, provide that the CA obtained the data or document from a source specified under Section 3.2 no more than thirty-nine (39) months prior to issuing the Certificate.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

No stipulation.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The CA maintains controls to provide reasonable assurance that, for domain validated certificates, Subscriber ’s certificate requests are accurate and complete.

The Certification Authority maintains effective controls to provide reasonable assurance that subordinate CA certificate requests are accurate, authenticated and approved.

4.1.1 Who can submit a certificate application

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

The CA MAY only issue EV Certificates to Applicants that meet the Private Organization, Government Entity, Business Entity and Non-Commercial Entity requirements specified below.

Issuers MAY only issue EV Code Signing Objects to Applicants that meet the requirements specified in Section 4.1 of the EV Code Signing Guidelines.

4.1.1.1 Private Organization Subjects

An Applicant qualifies as a Private Organization if:

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

4.1.1.2 Government Entity Subjects

An Applicant qualifies as a Government Entity if:

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

4.1.1.3 Business Entity Subjects

An Applicant qualifies as a Business Entity if:

1. The entity is a legally recognized entity that filed certain forms with a Registration Agency in its jurisdiction, the Registration Agency issued or approved the entity's charter, certificate, or license, and the entity's existence can be verified with that Registration Agency;
2. The entity has a verifiable physical existence and business presence;
3. At least one Principal Individual associated with the entity is identified and validated by the CA;
4. The identified Principal Individual attests to the representations made in the Subscriber Agreement;
5. the CA verifies the entity's use of any assumed name used to represent the entity pursuant to the requirements of EV Guidelines Section 11.3;
6. The entity and the identified Principal Individual associated with the entity are not located or residing in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and

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

4.1.1.4 Non-Commercial Entity Subjects

An Applicant qualifies as a Non-Commercial Entity if:

1. The Applicant is an International Organization, created under a charter, treaty, convention or equivalent instrument that was signed by, or on behalf of, more than one country's government. The CA/Browser Forum may publish a listing of Applicants who qualify as an International Organization for EV eligibility; and
2. The Applicant is not headquartered in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
3. The Applicant is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

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

4.1.2 Enrollment process and responsibilities

Prior to the issuance of a Certificate, the CA SHALL obtain the following documentation from the Applicant:

1. A certificate request, which may be electronic; and
2. An executed Subscriber Agreement or Terms of Use, which may be electronic.

The CA SHOULD obtain any additional documentation the CA determines necessary to meet these Requirements.

Prior to the issuance of a Certificate, the CA SHALL obtain from the Applicant a certificate request in a form prescribed by the CA and that complies with these Requirements. One 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 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 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.

4.1.2.1 Applicant roles

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

- Certificate Requester: The EV Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is an Individual 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 Approver: The EV Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is an Individual who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve EV Certificate Requests submitted by other Certificate Requesters.
- Contract Signer: A Subscriber Agreement applicable to the requested EV Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is an Individual who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.
- Applicant Representative: In the case where the CA and the Subscriber are affiliated, Terms of Use applicable to the requested EV Certificate MUST be acknowledged and agreed to by an authorized Applicant Representative. An Applicant Representative is a natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to acknowledge and agree to the Terms of Use.

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

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

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 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. The CA SHALL establish and follow 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 Fully-Qualified Domain Name or IP address to be included in the Certificate's SubjectAltName extension.

The CA 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 , the CA 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

The CA MAY delegate the performance of all or any part of a requirement of this CP to an Affiliate or a RA or subcontractor, provided that the process employed by the CA fulfills all of the requirements of EV Guidelines Section 11.13.

The CA MAY delegate the performance of all or any part of a requirement of this Certificate Policy to an Affiliate, a RA, or subcontractor, provided that the process employed by the CA fulfills all of the requirements of Section 11.12 of the EV Guidelines. Affiliates and/or RAs must comply with the qualification requirements of Sections 5.2.4, 5.3.2, 5.3.3.

The CA SHALL verify that the RA or subcontractor personnel involved in the issuance of a Certificate meet the training and skills requirements of Section 14 and the document retention and event logging requirements of Section 15.

4.2.2 Approval or rejection of certificate applications

CAs SHOULD NOT issue 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, the CA MUST provide a warning to the applicant that the gTLD may soon become resolvable and that, at that time, the CA 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 the CA 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 MUST (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 the CA 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], CAs MUST 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

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA maintains controls to provide reasonable assurance that certificates are generated and issued in accordance with the CA's disclosed business practices.

The Parent CA maintains controls to provide reasonable assurance that new, renewed and rekeyed Subordinate CA certificates are generated and issued in accordance with the CA's disclosed business practices.

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

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

1. Self-signed Certificates to represent the Root CA itself;
2. Certificates for Subordinate CAs and Cross Certificates;
3. Certificates for infrastructure purposes (e.g. administrative role certificates, internal CA operational device certificates, and OCSP Response verification Certificates);
4. Certificates issued solely for the purpose of testing products with Certificates issued by a Root CA; and
5. Subscriber Certificates, provided that: a. The Root CA uses a 1024-bit RSA signing key that was created prior to the Effective Date; b. The Applicant's application was deployed prior to the Effective Date; c. The Applicant's application is in active use by the Applicant or the CA uses a documented process to establish that the Certificate's use is required by a substantial number of Relying Parties; d. The CA follows a documented process to determine that the Applicant's application poses no known security risks to Relying Parties; and e. The CA documents that the Applicant's application cannot be patched or replaced without substantial economic outlay.

Root CA Private Keys MUST NOT be used to sign EV Certificates.

Issuance of an EV Code Signing Object SHALL require an individual authorized by the CA (i.e. the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command to perform a certificate signing operation. Root CA Private Keys MUST NOT be used to sign EV Code Signing Certificates or create EV Signatures.

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

The CA maintains controls to provide reasonable assurance that, upon issuance, complete and accurate certificates are available to subscribers and relying parties in accordance with the CA's disclosed business practices.

The Parent CA maintains controls to provide reasonable assurance that upon issuance, complete and accurate Subordinate CA certificates are available to relevant entities (Subscribers and Relying Parties) in accordance with the CA's disclosed business practices.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

The Certification Authority maintains effective controls to provide reasonable assurance that the integrity of subscriber keys and certificates it manages is established and protected throughout their life cycles

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

4.6.1 Circumstance for certificate renewal

No stipulation.

4.6.2 Who may request renewal

No stipulation.

4.6.3 Processing certificate renewal requests

The CA maintains controls to provide reasonable assurance that certificate renewal requests are accurate, authorized and complete.

The Parent CA maintains controls to provide reasonable assurance that subordinate CA certificate replacement (renewal and rekey) requests are accurate, authorized, and complete.

4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

4.6.6 Publication of the renewal certificate by the CA

No stipulation.

4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

The CA maintains controls to provide reasonable assurance that certificate rekey requests, including requests following certificate revocation or expiration, are accurate, authorized and complete.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

No stipulation.

4.7.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

4.8.2 Who may request certificate modification

No stipulation.

4.8.3 Processing certificate modification requests

No stipulation.

4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

4.8.6 Publication of the modified certificate by the CA

No stipulation.

4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

4.9 Certificate revocation and suspension

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

4.9.1 Circumstances for revocation

The Parent CA maintains controls to provide reasonable assurance that subordinate CA certificates are revoked based on authorized and validated certificate revocation requests.

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Certificate within 24 hours if one or more of the following occurs:

1. The Subscriber requests in writing that the CA revoke the Certificate;
2. The Subscriber notifies the CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The CA 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 Appendix A;
4. The CA obtains evidence that the Certificate was misused;
5. The CA is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
6. The CA is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
7. The CA is made aware that a Wildcard Certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
8. The CA is made aware of a material change in the information contained in the Certificate;
9. The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;

10. The CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
11. The CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
12. The CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the CA has made arrangements to continue maintaining the CRL/OCSP Repository;
13. The CA 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 the CA's Certificate Policy and/or Certification Practice Statement; or
15. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

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

Responsiveness. The CA SHALL respond to all plausible notices that a signed software object containing Suspect Code verifies with a certificate that it has issued by setting the revocation status of that certificate to 'revoked'.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

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

10. The technical content or format of the Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (e.g. the CA/Browser Forum might determine that a deprecated cryptographic/signature algorithm or key size presents an unacceptable risk and that such Certificates should be revoked and replaced by CAs within a given period of time).

4.9.2 Who can request revocation

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

4.9.3 Procedure for revocation request

The CA maintains controls to provide reasonable assurance that certificates are revoked, based on authorized and validated certificate revocation requests within the time frame in accordance with the CA's disclosed business practices.

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

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

The CA SHALL begin investigation of a Certificate Problem Report within twenty-four hours of receipt, and decide 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 (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
4. Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency (if applicable)

4.9.7.1 For the status of Subscriber Certificates

If the CA publishes a CRL, then the CA SHALL update and reissue CRLs at least once every seven days, and the value of the nextUpdate field MUST NOT be more than ten days beyond the value of the thisUpdate field

4.9.7.2 For the status of Subordinate CA Certificates

The CA SHALL update and reissue CRLs at least (i) once every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field MUST NOT be more than twelve months beyond the value of the thisUpdate field

4.9.8 Maximum latency for CRLs (if applicable)

The CA SHALL operate and maintain its CRL and OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

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

4.9.9 On-line revocation/status checking availability

OCSP responses MUST conform to RFC2560 and/or RFC5019. OCSP responses MUST either:

1. Be signed by the CA that issued the Certificates whose revocation status is being checked, or
2. Be signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

In the latter case, the OCSP signing Certificate MUST contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC2560.

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

4.9.10 On-line revocation checking requirements

The CA SHALL support 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 SHOULD NOT respond with a “good” status. The CA SHOULD monitor the responder for such requests as part of its security response procedures.

OCSP responders for CAs which are not Technically Constrained in line with Section 7.1.5 MUST NOT respond with a “good” status for such certificates.

4.9.10.1 For the status of Subscriber Certificates

The CA SHALL update information provided via an Online Certificate Status Protocol at least every four days. OCSP responses from this service MUST have a maximum expiration time of ten days.

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

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

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

4.9.10.2 For the status of Subordinate CA Certificates

The CA SHALL update information provided via an Online Certificate Status Protocol at least (i) every twelve months and (ii) within 24 hours after revoking a Subordinate CA Certificate.

4.9.11 Other forms of revocation advertisements available

If the Subscriber Certificate is for a high-traffic FQDN, the CA MAY rely on stapling, in accordance with [RFC4366], to distribute its OCSP responses. In this case, the CA SHALL ensure that the Subscriber "staples" the OCSP response for the Certificate in its TLS handshake. The CA SHALL enforce this requirement on the Subscriber either contractually, through the Subscriber Agreement or Terms of Use, or by technical review measures implemented by the CA.

4.9.12 Special requirements re key compromise

The CA maintains controls to provide reasonable assurance that continuity of operations is maintained in the event of the compromise of the CA's Private Keys and any certificates, signed with the compromised keys, are revoked and reissued.

4.9.13 Circumstances for suspension

The CA maintains controls to provide reasonable assurance that certificates are suspended based on authorized and validated certificate suspension requests within the time frame in accordance with the CA's disclosed business practices.

The Repository MUST NOT include entries that indicate that a Certificate is suspended.

4.9.14 Who can request suspension

No stipulation.

4.9.15 Procedure for suspension request

No stipulation.

4.9.16 Limits on suspension period

No stipulation.

4.10 Certificate status services

The CA maintains controls to provide reasonable assurance that timely, complete and accurate certificate status information (including Certificate Revocation Lists and other certificate status mechanisms) is made available to relevant entities (Subscribers and Relying Parties or their agents) in accordance with the CA's disclosed business practices.

4.10.1 Operational characteristics

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

4.10.2 Service availability

The CA SHALL maintain an online 24x7 Repository that application software can use to automatically check the current status of all unexpired Certificates issued by the CA.

The CA SHALL maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

If the CA provides subscriber (confidentiality) key storage, recovery or escrow services, the CA maintains controls to provide reasonable assurance that Subscriber Private Keys archived and escrowed by the CA remain confidential.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

The CA maintains controls to provide reasonable assurance that security is planned, managed and supported within the organization.

The CA maintains controls to provide reasonable assurance that security risks are identified and managed.

The CA maintains controls to provide reasonable assurance that the security of CA facilities, systems and information assets accessed by third parties is maintained.

The CA maintains controls to provide reasonable assurance that the security of Subscriber and Relying Party information is maintained when the responsibility for CA sub-functions has been outsourced to another organization or entity.

The CA must maintain controls to provide reasonable assurance that CA assets and Subscriber and Relying Party information receive an appropriate level of protection based upon identified risks and in accordance with the CA's disclosed business practices.

The CA SHALL develop, implement, and maintain a comprehensive security program designed to:

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

The Certificate Management Process MUST include:

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

The CA's security program MUST include an annual Risk Assessment that:

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

Based on the Risk Assessment, the CA SHALL develop, implement, and maintain a security plan consisting of security procedures, measures, and products designed to achieve the objectives set forth above and to manage and control the risks identified during the Risk Assessment, commensurate with the sensitivity of the Certificate Data and Certificate Management Processes. The security plan MUST include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and

Certificate Management Processes. The security plan MUST also take into account then-available technology and the cost of implementing the specific measures, and SHALL implement a reasonable level of security appropriate to the harm that might result from a breach of security and the nature of the data to be protected.

5.1 Physical controls

The CA maintains controls to provide reasonable assurance that CA facilities and equipment are protected from environmental hazards.

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

The CA maintains controls to provide reasonable assurance that physical access to CA facilities and equipment is limited to authorized individuals, protected through restricted security perimeters, and is operated under multiple person (at least dual custody) control.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

The CA must maintain controls to provide reasonable assurance that media are securely handled to protect them from damage, theft and unauthorized access.

5.1.7 Waste disposal

No stipulation.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

Each CA or Delegated Third Party SHALL document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed

Each CA or Delegated Third Party SHALL follow a documented procedure for appointing individuals to Trusted Roles and assigning responsibilities to them

Each CA or Delegated Third Party SHALL grant administration access to Certificate Systems only to persons acting in Trusted Roles and require their accountability for the Certificate System's security

5.2.2 Number of persons required per task

The Private Key SHALL be backed up, stored, and recovered only by personnel in trusted roles using, at least, dual control in a physically secured environment.

Systems used to process and approve EV Certificate Requests MUST require actions by at least two persons in Trusted Roles before creating an EV Certificate.

Systems used to process and approve EV Code Signing Certificate and EV Signature requests MUST require actions by at least two persons in Trusted Roles before creating an EV Code Signing Certificate or EV Signature.

5.2.3 Identification and authentication for each role

Each CA or Delegated Third Party SHALL require that each individual in a Trusted Role use a unique credential created by or assigned to that person in order to authenticate to Certificate Systems.

5.2.4 Roles requiring separation of duties

Each CA or Delegated Third Party SHALL document the responsibilities and tasks assigned to Trusted Roles and implement "separation of duties" for such Trusted Roles based on the security-related concerns of the functions to be performed.

The CA MUST enforce rigorous control procedures for the separation of validation duties to ensure that no one person can single-handedly validate and authorize the issuance of an EV Certificate. The Final Cross-Correlation and Due Diligence steps, as outlined in Section 11.13 of the EV Guidelines, MAY be performed by one of the persons. For example, one Validation Specialist MAY review and verify all the Applicant information and a second Validation Specialist MAY approve issuance of the EV Certificate.

5.3 Personnel controls

The CA must maintain controls to provide reasonable assurance that personnel and employment practices enhance and support the trustworthiness of the CA's operations.

5.3.1 Qualifications, experience, and clearance requirements

Prior to the engagement of any person in the Certificate Management Process, whether as an employee, agent, or an independent contractor of the CA, the CA SHALL verify the identity and trustworthiness of such person.

5.3.2 Background check procedures

Prior to the commencement of employment of any person by the CA for engagement in the EV Processes, whether as an employee, agent, or an independent contractor of the CA, the CA MUST:

1. **Verify the Identity of Such Person**: Verification of identity MUST be performed through:

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

and

1. **Verify the Trustworthiness of Such Person**: Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:

    A. Confirmation of previous employment,
    B. Check of professional references; 3.Confirmation of the highest or most-relevant educational qualification obtained; 4.Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed;

5.3.3 Training requirements

The CA SHALL provide all personnel performing information verification duties with skills-training that covers basic Public Key Infrastructure knowledge, authentication and vetting policies and procedures (including the CA's Certificate Policy and/or Certification Practice Statement), common threats to the information verification process (including phishing and other social engineering tactics), and these Requirements.

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

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

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

The required internal examination must relate to the EV Certificate validation criteria outlined in this Certificate Policy.

5.3.4 Retraining frequency and requirements

Validation Specialists engaged in Certificate issuance SHALL maintain skill levels consistent with the CA's training and performance programs.

5.3.5 Job rotation frequency and sequence

5.3.6 Sanctions for unauthorized actions

The CA must maintain controls to provide reasonable assurance that compliance with the CA's security policies and procedures is ensured.

Each CA or Delegated Third Party SHALL ensure that an individual in a Trusted Role acts only within the scope of such role when performing administrative tasks assigned to that role.

5.3.7 Independent contractor requirements

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

The CA is responsible for all tasks performed by Delegated Third Parties and Trusted Roles, and the CA SHALL define, document, and disclose to its auditors (a) the tasks assigned to Delegated Third Parties or Trusted Roles, and (b) the arrangements made with Delegated Third parties to ensure compliance with these Requirements, and (c) the relevant practices implemented by Delegated Third Parties.

The CA SHALL, for each Delegated Third Party, (i) require multi-factor authentication prior to the Delegated Third Party approving issuance of a Certificate or (ii) implement technical controls that restrict the Delegated Third Party's ability to approve certificate issuance to a limited set of Domain Names.

5.3.8 Documentation supplied to personnel

5.4 Audit logging procedures

The CA maintains controls to provide reasonable assurance that the effectiveness of the system audit process is maximized and interference to and from the system audit process is minimized.

The CA maintains controls to provide reasonable assurance that unauthorized CA system usage is detected.

5.4.1 Types of events recorded

The CA must maintain controls to provide reasonable assurance that significant CA environmental, key management, and certificate management events are accurately and appropriately logged.

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

The CA SHALL record at least the following events:

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

Log entries MUST include the following elements:

1. Date and time of entry;
2. Identity of the person making the journal entry; and
3. Description of the entry.

5.4.2 Frequency of processing log

The CA must maintain controls to provide reasonable assurance that audit logs are reviewed periodically by authorized personnel.

Certification Authorities and Delegated Third Parties SHALL conduct a human review of application and system logs at least every 30 days and validate the integrity of logging processes and ensure that monitoring, logging, alerting, and log-integrity verification functions are operating properly (the CA or Delegated Third Party MAY use an in-house or third-party audit log reduction and analysis tool).

5.4.3 Retention period for audit log

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

5.4.4 Protection of audit log

The CA must maintain controls to provide reasonable assurance that the confidentiality and integrity of current and archived audit logs are maintained.

5.4.5 Audit log backup procedures

The CA must maintain controls to provide reasonable assurance that audit logs are completely and confidentially archived in accordance with disclosed business practices.

5.4.6 Audit collection system (internal vs. external)

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Additionally, the CA's security program MUST include an annual Risk Assessment that:

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

Certification Authorities and Delegated Third Parties SHALL document and follow a vulnerability correction process that addresses the identification, review, response, and remediation of vulnerabilities

Certification Authorities and Delegated Third Parties SHALL undergo or perform a Vulnerability Scan (i) within one week of receiving a request from the CA/Browser Forum, (ii) after any system or network changes that the CA determines are significant, and (iii) at least once per quarter, on public and private IP addresses identified by the CA or Delegated Third Party as the CA's or Delegated Third Party's Certificate Systems

5.5 Records archival

5.5.1 Types of records archived

Certification Authorities and Delegated Third Parties SHALL maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation.

Certification Authorities and Delegated Third Parties SHALL maintain, archive, and retain logs in accordance with disclosed business practices and applicable legislation.

5.5.2 Retention period for archive

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

5.5.3 Protection of archive

No stipulation.

5.5.4 Archive backup procedures

No stipulation.

5.5.5 Requirements for time-stamping of records

No stipulation.

5.5.6 Archive collection system (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

No stipulation.

5.7 Compromise and disaster recovery

The CA must maintain controls to provide reasonable assurance that loss, damage or compromise of assets and interruption to business activities are prevented.

The CA maintains controls to provide reasonable assurance of continuity of operations in the event of a disaster.

The CA maintains controls to provide reasonable assurance of the development and testing of a CA business continuity plan that includes a disaster recovery process for critical components of the CA system.

The CA maintains controls to provide reasonable assurance of storage of required cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location.

The CA maintains controls to provide reasonable assurance of the storage backups of systems, data and configuration information at an alternate location.

The CA maintains controls to provide reasonable assurance of the availability of an alternate site, equipment and connectivity to enable recovery.

The CA maintains controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.

5.7.1 Incident and compromise handling procedures

The CA must maintain controls to provide reasonable assurance that damage from security incidents and malfunctions is minimized through the use of incident reporting and response procedures.

The CA SHALL document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The CA is not required to publicly disclose its business continuity plans but SHALL make its business continuity plan and security plans available to the CA's auditors upon request. The CA SHALL annually test, review, and update these procedures.

The business continuity plan MUST include:

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

5.7.2 Computing resources, software, and/or data are corrupted

No stipulation.

5.7.3 Entity private key compromise procedures

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

5.8 CA or RA termination

The CA must maintain controls to provide reasonable assurance that potential disruptions to Subscribers and Relying Parties are minimized as a result of the cessation or degradation of the CA's services.

6 TECHNICAL SECURITY CONTROLS

The CA maintains controls to provide reasonable assurance that the correct and secure operation of CA information processing facilities is ensured.

6.1 Key pair generation and installation

The CA must maintain controls to provide reasonable assurance that CA key pairs are generated in accordance with the CA's disclosed business practices and defined procedures specified within detailed key generation ceremony scripts.

6.1.1 Key pair generation

6.1.1.1 CA Key Pair Generation

The CA maintains controls to provide reasonable assurance that the CA's disclosed business practices include generation of CA keys are undertaken in a physically secured environment.

The CA maintains controls to provide reasonable assurance that the CA's disclosed business practices include generation of CA keys are performed by personnel in Trusted Roles under the principles of multiple person control and split knowledge.

The CA maintains controls to provide reasonable assurance that the CA's disclosed business practices include generation of CA keys occur within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CPS.

The CA maintains controls to provide reasonable assurance that the CA's disclosed business practices include generation of CA keys are witnessed by an independent party and/or videotaped.

The CA maintains controls to provide reasonable assurance that the CA's disclosed business practices include CA key generation activities are logged.

The CA key generation script includes the following:

- definition of roles and participant responsibilities;
- approval for conduct of the key generation ceremony;
- cryptographic hardware and activation materials required for the ceremony;
- specific steps performed during the key generation ceremony;
- physical security requirements for the ceremony location;
- procedures for secure storage of cryptographic hardware and activation materials following the key generation ceremony;
- sign-off from participants and witnesses indicating whether key generation ceremony was performed in accordance with the detailed key generation ceremony script; and
- notation of any deviations from the key generation ceremony script.

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

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

For other CA Key Pairs created after the Effective Date that are for the operator of the Root CA or an Affiliate of the Root CA, the CA SHOULD:

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

In all cases, the CA SHALL:

1. generate the keys in a physically secured environment as described in the CA's Certification Practice Statement;
2. generate the CA keys using personnel in Trusted Roles under the principles of multiple person control and split knowledge;
3. generate the CA keys within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's Certification Practice Statement;
4. log its CA key generation activities; and
5. maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its Certification Practice Statement and (if applicable) its Key Generation Script.

For Root CA Key Pairs used for EV Certificates which are generated after the release of this Certificate Policy, the Root CA Key Pair generation ceremony MUST be witnessed by the CA's Qualified Auditor in order to observe the process and the controls over the integrity and confidentiality of the Root CA Key Pairs produced. The Qualified Auditor MUST then issue a report opining that the CA, during its Root CA Key Pair and Certificate generation process:

1. Documented its Root CA key generation and protection procedures in its Certificate Policy, and its Certification Practices Statement;
2. Included appropriate detail in its Root Key Generation Script;
3. Maintained effective controls to provide reasonable assurance that the Root CA key pair was generated and protected in conformity with the procedures described in its CP/CPS and with its Root Key Generation Script;
4. Performed, during the Root CA key generation process, all the procedures required by its Root Key Generation Script.

6.1.1.2 RA Key Pair Generation

No stipulation.

6.1.1.3 Subscriber Key Pair Generation

If the CA provides Subscriber key management services, the CA maintains controls to provide reasonable assurance that subscriber keys generated by the CA (or RA or card bureau) are generated within a secure cryptographic device based on a risk assessment and the business requirements of the CA in accordance with the CA's disclosed business practices.

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in Appendix A or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys (http://wiki.debian.org/SSLkeys)).

6.1.2 Private key delivery to subscriber

If the CA provides Subscriber key management services, the CA maintains controls to provide reasonable assurance that subscriber keys generated by the CA (or RA or card bureau) are securely distributed to the subscriber by the CA (or RA or card bureau) in accordance with the CA's disclosed business practices.

If the CA (or RA) distributes subscriber key pairs and certificates using ICCs, the CA (or RA) maintains controls to provide reasonable assurance that:

- ICC procurement, preparation and personalization are securely controlled by the CA (or RA or card bureau);
- ICC ADF preparation is securely controlled by the CA (or RA);
- ICC usage is enabled by the CA (or RA or card bureau) prior to ICC issuance;
- ICC deactivation and reactivation are securely controlled by the CA (or RA);
- ICCs are securely stored and distributed by the CA (or RA or card bureau);
- ICCs are securely replaced by the CA (or RA or card bureau); and
- ICCs returned to the CA (or RA or card bureau) are securely terminated.

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.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

The CA must maintain controls to provide reasonable assurance that the integrity and authenticity of the CA public keys and any associated parameters are maintained during initial and subsequent distribution.

6.1.5 Key sizes

Certificates MUST meet the following requirements for algorithm type and key size.

For DSA keys, L and N (the bit lengths of modulus p and divisor q, respectively) are described in the Digital Signature Standard, FIPS 186-3 (http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf (http://csrc.nist.gov/publications/fips/fips186-3/fips_186-3.pdf)).

6.1.5.1 Root CA Certificates

	Validity period beginning on or before 31 Dec 2010	Validity period beginning after 31 Dec 2010
Digest algorithm	MD5 (NOT RECOMMENDED), SHA-1, SHA-256, SHA-384 or SHA-512	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048**	2048
ECC curve	NIST P-256, P-384, or P-521	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048 N= 224 or L= 2048 N= 256	L= 2048 N= 224 or L= 2048 N= 256

* SHA-1 MAY be used with RSA keys until SHA-256 is supported widely by browsers used by a substantial portion of relying-parties worldwide.

** 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.

6.1.5.2 Subordinate CA Certificates

Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048 N= 224 or L= 2048 N= 256

6.1.5.3 Subscriber Certificates

Digest algorithm	SHA-1*, SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	2048
ECC curve	NIST P-256, P-384, or P-521
Minimum DSA modulus and divisor size (bits)	L= 2048 N= 224 or L= 2048 N= 256

6.1.6 Public key parameters generation and quality checking

RSA: The CA 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. The CA 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: The CA 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 5.6.2.5 and 5.6.2.6, respectively, NIST SP 800-56A]

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA must maintain controls to provide reasonable assurance that CA keys are used only for their intended functions in their predetermined locations.

The CA maintains controls to provide reasonable assurance that any Subscriber key management tools provided by the CA support the requirements of the CA's business practices disclosure.

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the Private Key outside the validated system or device specified above MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key. The CA SHALL encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

The CA maintains controls to provide reasonable assurance that devices used for private key storage and recovery and the interfaces to these devices are tested before usage for integrity.

The CA maintains controls to provide reasonable assurance that access to CA cryptographic hardware is limited to authorized personnel in trusted roles, using multiple person control.

The CA maintains controls to provide reasonable assurance that CA cryptographic hardware is functioning correctly.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

The CA maintains controls to provide reasonable assurance that escrowed CA private signing keys remain confidential.

6.2.4 Private key backup

No stipulation.

6.2.5 Private key archival

The CA maintains controls to provide reasonable assurance that archived CA keys remain confidential and secured and are never put back into production.

Parties other than the Subordinate CA SHALL NOT archive the Subordinate CA Private Keys.

6.2.6 Private key transfer into or from a cryptographic module

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

6.2.7 Private key storage on cryptographic module

The CA must maintain controls to provide reasonable assurance that CA private keys remain confidential and maintain their integrity. The CA's private keys are backed up, stored and recovered by authorized personnel in trusted roles, using multiple person control in a physically secured environment.

If the CA provides subscriber (confidentiality) key storage, recovery or escrow services, the CA maintains controls to provide reasonable assurance that subscriber private keys stored by the CA remain confidential and maintain their integrity.

The CA SHALL protect its Private Key in a system or device that has been validated as meeting at least FIPS 140 level 3 or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

An EV Timestamp Authority MUST protect its Private Key in a crypto module validated in accordance with FIPS 140-2 Level 2.

Signing Authorities shall protect private keys in a FIPS 140-2 level 2 (or equivalent) crypto module. Techniques that may be used to satisfy this requirement include:

a. Use of an HSM, verified by means of a manufacturer's certificate;
b. A hardware crypto module provided by the CA;
c. Contractual terms in the subscriber agreement requiring the Subscriber to protect the private key to a standard equivalent to FIPS 140-2 and with compliance being confirmed by means of an audit.
d. Cryptographic algorithms, key sizes and certificate life-times for both authorities and Subscribers are governed by the NIST key management guidelines.

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

a. The CA ships a suitable hardware crypto module, with a preinstalled key pair, in the form of a smartcard or USB device or similar;
b. The Subscriber counter-signs certificate requests that can be verified by using a manufacturer's certificate indicating that the key is managed in a suitable hardware module;
c. The Subscriber provides a suitable IT audit indicating that its operating environment achieves a level of security at least equivalent to that of FIPS 140-2 level 2.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

The CA maintains controls to provide reasonable assurance that CA keys are completely destroyed at the end of the Key Pair life cycle in accordance with the CA's disclosed business practices.

If the CA provides subscriber (confidentiality) key storage, recovery or escrow services, the CA maintains controls to provide reasonable assurance that Subscriber Private Keys stored by the CA are completely destroyed at the end of the Key Pair life cycle.

6.2.11 Cryptographic Module Rating

No stipulation.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No stipulation.

6.3.2 Certificate operational periods and key pair usage periods

Subscriber Certificates issued after the Effective Date MUST have a Validity Period no greater than 60 months. Except as provided for below, Subscriber Certificates MUST have a Validity Period no greater than 39 months.

CAs MAY continue to issue Subscriber Certificates with a Validity Period greater than 39 months but not greater than 60 months provided that the CA documents that the Certificate is for a system or software that:

(a) was in use prior to the Effective Date; (b) is currently in use by either the Applicant or a substantial number of Relying Parties; (c) fails to operate if the Validity Period is shorter than 60 months; (d) does not contain known security risks to Relying Parties; and (e) is difficult to patch or replace without substantial economic outlay.

The validity period for an EV Certificate SHALL NOT exceed twenty seven months. It is RECOMMENDED that EV Subscriber Certificates have a maximum validity period of twelve months.

Code may be signed at any point in the development or distribution process, either by a software publisher or a user organization.

Signed code may be verified at any time, including during: download, unpacking, installation, reinstallation, or execution, or during a forensic investigation.

Subscribers may obtain an EV Code Signing Certificate with a validity period not exceeding thirty-nine months.

Timestamp Authorities and Signing Authorities may obtain an EV Timestamp Certificate or EV Code Signing Certificate (respectively) with a validity period not exceeding one hundred and twenty three months.

The validity period for an EV Code Signing Certificate issued to a Subscriber MUST NOT exceed thirty-nine months. The validity period for an EV Code Signing Certificate issued to a Signing Authority that fully complies with this Certificate Policy MUST NOT exceed one hundred and twenty three months. The validity period for an EV Timestamp Certificate issued to a Timestamp Authority that fully complies with this Certificate Policy MUST NOT exceed one hundred and twenty three months.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

The CA must maintain controls to provide reasonable assurance that compromise of information and information processing facilities is prevented.

The CA must maintain controls to provide reasonable assurance that CA system access is limited to authorized individuals.

The CA must maintain controls to provide reasonable assurance that the risk of CA systems failure is minimized.

The CA maintains controls to provide reasonable assurance that operating system and database access is limited to authorized individuals with predetermined task privileges.

6.5.1 Specific computer security technical requirements

The CA maintains controls to provide reasonable assurance that CA application use is limited to authorized individuals.

6.5.1.1 Account Management

The CA SHALL enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

Each CA or Delegated Third Party SHALL change authentication keys and passwords for any privileged account or service account on a Certificate System whenever a person's authorization to administratively access that account on the Certificate System is changed or revoked.

Each CA or Delegated Third Party SHALL review all system accounts at least every 90 days and deactivate any accounts that are no longer necessary for operations.

Each CA or Delegated Third Party SHALL implement a process that disables all privileged access of an individual to Certificate Systems within 24 hours upon termination of the individual's employment or contracting relationship with the CA or Delegated Third Party.

Each CA or Delegated Third Party SHALL enforce multi-factor authentication for administrator access to Issuing Systems and Certificate Management Systems.

6.5.1.2 Least Privilege

Each CA or Delegated Third Party SHALL require employees and contractors to observe the principle of "least privilege" when accessing, or when configuring access privileges on, Certificate Systems.

6.5.1.3 Access Control Best Practices

Each CA or Delegated Third Party SHALL require Trusted Roles to log out of or lock workstations when no longer in use.

Each CA or Delegated Third Party SHALL configure workstations with inactivity time-outs that log the user off or lock the workstation after a set time of inactivity without input from the user (the CA or Delegated Third Party MAY allow a workstation to remain active and unattended if the workstation is otherwise secured and running administrative tasks that would be interrupted by an inactivity time-out or system lock).

6.5.1.4 Authentication: Passwords and Accounts

If an authentication control used by a Trusted Role is a username and password, then, where technically feasible, each CA or Delegated Third Party SHALL implement the following controls:

1. For accounts that are not publicly accessible (accessible only within Secure Zones or High Security Zones), require that passwords have at least twelve (12) characters;
2. For accounts that are accessible from outside a Secure Zone or High Security Zone, require that passwords have at least eight (8) characters, be changed at least every 90 days, use a combination of at least numeric and alphabetic characters, that are not a dictionary word or on a list of previously disclosed human-generated passwords, and not be one of the user's previous four passwords; and implement account lockout for failed access attempts in accordance with subsection k; OR
3. Implement a documented password management and account lockout policy that the CA has determined provide at least the same amount of protection against password guessing as the foregoing controls.

Each CA or Delegated Third Party SHALL lockout account access to Certificate Systems after no more than five (5) failed access attempts, provided that this security measure is supported by the Certificate System and does not weaken the security of this authentication control.

6.5.1.5 System Isolation and Partitioning

Each CA or Delegated Third Party SHALL segment Certificate Systems into networks or zones based on their functional, logical, and physical (including location) relationship.

6.5.1.6 Malicious Code Protection

The CA maintains controls to provide reasonable assurance that the integrity of CA systems and information is protected against viruses and malicious software.

Certification Authorities and Delegated Third Parties SHALL implement detection and prevention controls under the control of CA or Delegated Third Party Trusted Roles to protect Certificate Systems against viruses and malicious software.

6.5.1.7 Software and Firmware Integrity

Certification Authorities and Delegated Third Parties SHALL implement a Security Support System under the control of CA or Delegated Third Party Trusted Roles that monitors, detects, and reports any security-related configuration change to Certificate Systems.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

The CA must maintain controls to provide reasonable assurance that CA systems development and maintenance activities are documented, tested, authorized, and properly implemented to maintain CA system integrity.

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

Each CA or Delegated Third Party SHALL apply recommended security patches to Certificate Systems within six months of the security patch's availability, unless the CA documents that the security patch would introduce additional vulnerabilities or instabilities that outweigh the benefits of applying the security patch.

Each CA or Delegated Third Party SHALL do one of the following within 96 hours of discovery of a Critical Vulnerability not previously addressed by the CA's vulnerability correction process:

1. Remediate the Critical Vulnerability;
2. If remediation of the Critical Vulnerability within 96 hours is not possible, create and implement a plan to mitigate the Critical Vulnerability, giving priority to (1) vulnerabilities with high CVSS scores, starting with the vulnerabilities the CA determines are the most critical (such as those with a CVSS score of 10.0) and (2) systems that lack sufficient compensating controls that, if the vulnerability were left unmitigated, would allow external system control, code execution, privilege escalation, or system compromise; or
3. Document the factual basis for the CA's determination that the vulnerability does not require remediation because (a) the CA disagrees with the NVD rating, (b) the identification is a false positive, (c) the exploit of the vulnerability is prevented by compensating controls or an absence of threats; or (d) other similar reasons

6.7 Network security controls

6.7.1 Boundary Systems

Each CA or Delegated Third Party SHALL apply the same security controls to all systems co-located in the same zone with a Certificate System.

6.7.1.1 PKI Network Zones Overview

Each CA or Delegated Third Party SHALL maintain Root CA Systems in a High Security Zone and in an offline state or air-gapped from all other networks.

Each CA or Delegated Third Party SHALL maintain and protect Issuing Systems, Certificate Management Systems, and Security Support Systems in at least a Secure Zone.

6.7.1.2 Special Access Zone Boundary

The CA must maintain controls to provide reasonable assurance that access to network segments housing CA systems is limited to authorized individuals, applications and services.

Each CA or Delegated Third Party SHALL ensure that only personnel assigned to Trusted Roles have access to Secure Zones and High Security Zones.

6.7.1.3 Restricted Zone Boundary

Each CA or Delegated Third Party SHALL configure each network boundary control (firewall, switch, router, gateway, or other network control device or system) with rules that support only the services, protocols, ports, and communications that the CA has identified as necessary to its operations.

Each CA or Delegated Third Party SHALL configure Issuing Systems, Certificate Management Systems, Security Support Systems, and Front-End / Internal-Support Systems by removing or disabling all accounts, applications, services, protocols, and ports that are not used in the CA's or Delegated Third Party's operations and allowing only those that are approved by the CA or Delegated Third Party.

6.7.1.4 Operational Zone Boundary

Each CA or Delegated Third Party SHALL implement and configure Security Support Systems that protect systems and communications between systems inside Secure Zones and High Security Zones, and communications with non-Certificate Systems outside those zones (including those with organizational business units that do not provide PKI-related services) and those on public networks.

6.7.2 Network Monitoring

Each CA or Delegated Third Party SHALL implement automated mechanisms under the control of CA or Delegated Third Party Trusted Roles to process logged system activity and alert personnel, using notices provided to multiple destinations, of possible Critical Security Events.

6.7.2.1 Monitoring devices

Each CA or Delegated Third Party SHALL identify those Certificate Systems under the control of CA or Delegated Third Party Trusted Roles capable of monitoring and logging system activity and enable those systems to continuously monitor and log system activity

6.7.2.2 Monitoring of Security Alerts, Advisories, and Directives

Each CA or Delegated Third Party SHALL require Trusted Role personnel to follow up on alerts of possible Critical Security Events.

6.7.3 Remote Access/External Information Systems

Each CA or Delegated Third Party SHALL restrict remote administration or access to an Issuing System, Certificate Management System, or Security Support System except when: (i) the remote connection originates from a device owned or controlled by the CA or Delegated Third Party and from a pre-approved external IP address, (ii) the remote connection is through a temporary, non-persistent encrypted channel that is supported by multi-factor authentication, and (iii) the remote connection is made to a designated intermediary device (a) located within the CA's network, (b) secured in accordance with these Requirements, and (c) that mediates the remote connection to the Issuing System.

6.7.4 Penetration Testing

Each CA or Delegated Third Party SHALL undergo a Penetration Test on the CA's and each Delegated Third Party's Certificate Systems on at least an annual basis and after infrastructure or application upgrades or modifications that the CA determines are significant.

Each CA or Delegated Third Party SHALL record evidence that each Vulnerability Scan and Penetration Test was performed by a person or entity (or collective group thereof) with the skills, tools, proficiency, code of ethics, and independence necessary to provide a reliable Vulnerability Scan or Penetration Test.

6.8 Time-stamping

An EV Timestamp Authority MUST be synchronized with a UTC(k) time source recognized by the BIPM.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The CA SHALL meet the technical requirements set forth in Section 2.2 – Publication of Information, Section 7.1.2 - Certificate Extensions, Section 6.1.5- Key Sizes, and Section 6.1.6 - Public Key Parameters Generation and Quality Checking.

CAs SHALL generate non-sequential Certificate serial numbers greater than zero (0) containing at least 64 bits of output from a CSPRNG.

7.1.1 Version number(s)

Certificates MUST be of type X.509 v3.

7.1.2 Certificate extensions

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1 Root CA Certificate

- basicConstraints This extension MUST appear as a critical extension. The cA field MUST be set true. The pathLenConstraint field SHOULD NOT be present.

- keyUsage This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- certificatePolicies This extension SHOULD NOT be present.
- extendedKeyUsage This extension MUST NOT be present.

7.1.2.2 Subordinate CA Certificate

- certificatePolicies This extension MUST be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (Required)

The following fields MAY be present if the Subordinate CA is not an Affiliate of the entity that controls the Root CA.

** certificatePolicies:policyQualifiers:policyQualifierId (Optional)

id-qt 1 [RFC 5280].

** certificatePolicies:policyQualifiers:qualifier:cPSuri (Optional)

HTTP URL for the Root CA's Certificate Policy, Certification Practice Statement, Relying Party Agreement, or other pointer to online policy information provided by the CA.

- cRLDistributionPoints This extension MUST be present and MUST NOT be marked critical. It MUST contain the HTTP URL of the CA's CRL service.
- authorityInformationAccess With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and 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" the OCSP response for the Certificate in its TLS handshakes [RFC4366].

- basicConstraints This extension MUST be present and MUST be marked critical. The cA field MUST be set true. The pathLenConstraint field MAY be present.
- keyUsage This extension MUST be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign MUST be set. If the Subordinate CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.
- nameConstraints (optional) If present, this extension SHOULD be marked critical*.

* 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.

- extkeyUsage (optional) For Subordinate CA Certificates to be Technically constrained in line with section 7.1.5, then either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values MUST be present**.

Other values MAY be present.

If present, this extension SHOULD be marked non-critical.

** 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.

For EV Certificates:

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

- certificatePolicies:policyQualifiers:policyQualifierId
    - id-qt 1 [RFC 5280]
- certificatePolicies:policyQualifiers:qualifier:cPSuri
    - HTTP URL for the Root CA's Certification Practice Statement

7.1.2.3 Subscriber Certificate

- certificatePolicies This extension MUST be present and SHOULD NOT be marked critical.

** certificatePolicies:policyIdentifier (Required)

A Policy Identifier, defined by the issuing CA, that indicates a Certificate Policy asserting the issuing CA's adherence to and compliance with these Requirements.

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 Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

- cRLDistributionPoints This extension MAY be present. If present, it MUST NOT be marked critical, and it MUST contain the HTTP URL of the CA's CRL service.

- authorityInformationAccess With the exception of stapling, which is noted below, this extension MUST be present. It MUST NOT be marked critical, and 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].

- basicConstraints (optional) If present, the cA field MUST be set false.

- keyUsage (optional) If present, bit positions for keyCertSign and cRLSign MUST NOT be set.

- extKeyUsage (required) 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.

The certificatePolicies extension in EV Certificates issued to Subscribers MUST include the following:

- certificatePolicies:policyIdentifier (Required)
    - The Issuer's EV policy identifier
- certificatePolicies:policyQualifiers:policyQualifierId (Required)
    - id-qt 1 [RFC 5280]
- certificatePolicies:policyQualifiers:qualifier:cPSuri (Required)
    - HTTP URL for the Subordinate CA's Certification Practice Statement

For EV Certificates, the cRLDistribution Point extension MUST be present in Subscriber Certificates if the certificate does not specify OCSP responder locations in an authorityInformationAccess extension

For EV Code Signing certificates:

As specified in Section 7.1.2.2, with the following exceptions:

A. the Domain Name required by Section 7.1.4.2 SHALL be omitted;

B. the Certificate MUST include a SubjectAltName:permanentIdentifier which MUST contain the following:

    1. The ISO 3166-2 country code corresponding Subject's Jurisdiction of Incorporation or Jurisdiction of Registration (CC), as specified in the subject:jurisdictionOfIncorporationCountryName field;
    2. If applicable, the state, province, or locality of the Subject's Jurisdiction of Incorporation in uppercase characters as specified in the subjectjurisdictionOfIncorporationLocalityName or subject:jurisdictionofIncorporationStateorProvinceName field, expressed in an unabbreviated format (STATE);

3. The first one of the following that applies:

    a. The Registration Number as included in the Subject:serialNumber field (REG),
    b. A date of Incorporation or Registration in YYYY-MM-DD format (DATE) and the Subject's Organization Name as included in the organizationName field (ORG),
    c. A verifiable date of creation in YYYY-MM-DD format (DATE) and the Subject's Organization Name as included in the organizationName field (ORG), or
    d. the Subject's Organization Name as included in the organizationName field (O).

   The CA SHALL format data in the SubjectAltName:permanentIdentifier extension using Unicode as follows: CC-STATE (if applicable)- REG or DATE (if available)-ORG (if REG is not present). Characters representing the organization name MUST be uppercase Unicode. Any included "-" characters MUST be Unicode 002D and any included spaces in REG, STATE, or ORG MUST be Unicode 0020.

   A CA MAY truncate or abbreviate an organization name included in this field to ensure that the combination does not exceed 64 characters provided that the CA checks this field in accordance with section 3.2 and a Relying Party will not be misled into thinking that they are dealing with a different organization. If this is not possible, the CA MUST NOT issue the EV Code Signing Certificate.

C. the keyUsage extension MUST be set as follows: This extension MUST be present and MUST be marked critical. The bit position for digitalSignature MUST be set. All other bit positions SHOULD NOT be set; AND
D. the extended keyUsage extension MUST be set as follows: This extension MUST be present, and the value id-kp-codeSigning MUST be present. Other values SHOULD NOT be present.

7.1.2.4 All Certificates

All other fields and extensions MUST be set in accordance with RFC 5280. The CA SHALL NOT issue a Certificate that contains a keyUsage flag, extendedKeyUsage value, Certificate extension, or other data not specified in this Appendix B unless the CA is aware of a reason for including the data in the Certificate.

CAs SHALL NOT issue a Certificate with:

a. Extensions that do not apply in the context of the public Internet (such as an extendedKeyUsage value for a service that is only valid in the context of a privately managed network), 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 the CA (such as including extendedKeyUsage value for a smart card, where the CA is not able to verify that the corresponding Private Key is confined to such hardware due to remote issuance).

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 Requirements.

7.1.3 Algorithm object identifiers

Effective 1 January 2016, CAs MUST NOT issue any new Subscriber certificates or Subordinate CA certificates using the SHA-1 hash algorithm. CAs MAY continue to sign certificates to verify OCSP responses using SHA1 until 1 January 2017. This Section 9.4.2 does not apply to Root CA or CA cross certificates. CAs MAY continue to use their existing SHA-1 Root Certificates. SHA-2 Subscriber certificates SHOULD NOT chain up to a SHA-1Subordinate CA Certificate.

CAs SHOULD NOT issue Subscriber Certificates utilizing the SHA-1 algorithm with an Expiry Date greater than 1 January 2017 because Application Software Providers are in the process of deprecating and/or removing the SHA-1 algorithm from their software, and they have communicated that CAs and Subscribers using such certificates do so at their own risk.

7.1.4 Name forms

Certificates names include Issuer Distinguished Name, Subject Distinguished Name, and Subject Alternative Name.

Name chaining is performed by matching the issuer distinguished name in one certificate with the subject name in a CA certificate.

7.1.4.1 Issuing CA Certificate Subject

An Issuing CA SHALL populate the Subject distinguished name of each Issuing CA Certificate issued after the adoption of these Requirements in accordance with the following table.

Relative Distinguished Name Type	**Required/ Optional**	**Contents**
commonName (OID 2.5.4.3)	Optional	If present in a Certificate, the Common Name field MUST include a name that accurately identifies the Issuing CA.
domainComponent (OID 0.9.2342.19200300.100.1.25)	Optional	If present in a Certificate, the Domain Component field MUST include all components of the Issuing CA's Registered Domain Name in ordered sequence, with the most significant component, closest to the root of the namespace, written last.
organizationName (OID 2.5.4.10)	Required	This field MUST contain the name (or abbreviation thereof), trademark, or other meaningful identifier for the CA, provided that they accurately identify the CA. The field MUST NOT contain a generic designation such as "Root" or "CA1".
countryName (OID 2.5.4.6)	Required	This field MUST contain the two-letter ISO 3166-1 country code for the country in which the issuer's place of business is located.

By issuing a Subordinate CA Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.2 Subject Information for Standard Server Authentication certificates

By issuing the Certificate, the CA represents that it followed the procedure set forth in its Certificate Policy and/or Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate. CAs SHALL NOT include a Domain Name in a Subject attribute except as specified below.

An Issuing CA SHALL populate the Subject distinguished name of each Certificate issued after the adoption of these Requirements in accordance with the following table.

Relative Distinguished Name Type	**Required/Optional**	**Contents**
commonName (OID 2.5.4.3)	Deprecated (Discouraged, but not prohibited)	If present, this field MUST contain a single IP address or Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.3).
domainComponent (OID 0.9.2342.19200300.100.1.25)	Optional.	If present, this field MUST contain a label from a Domain Name. The domainComponent fields for each Domain Name MUST be in a single ordered sequence containing all labels from the Domain name. The labels MUST be encoded in the reverse order to the on-wire representation of domain names in the DNS protocol, so that the label closest to the root is encoded first. The CA MUST ensure that the certificate is issued with the consent of, and according to procedures established by, the owner of each Domain Name.

Relative Distinguished Name Type	Required/Optional	Contents
organizationName (OID 2.5.4.10)	Optional.	If present, the subject:organizationName field MUST contain either the Subject's name or DBA as verified under Section 11.2. The CA may include information in this field that differs slightly from the verified name, such as common variations or abbreviations, provided that the CA documents the difference and any abbreviations used are locally accepted abbreviations; e.g., if the official record shows "Company Name Incorporated", the CA MAY use "Company Name Inc." or "Company Name". 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 organizationName field to convey a natural person Subject's name or DBA.
Number and street: streetAddress (OID: 2.5.4.9)	Optional if the subject:organizationName field is present. Prohibited if the subject:organizationName field is absent.	If present, the subject:streetAddress field MUST contain the Subject's street address information as verified under Section 11.2.
localityName (OID: 2.5.4.7)	Required if the subject:organizationName field is present and the subject:stateOrProvinceName field is absent. Optional if the subject:organizationName and subject:stateOrProvinceName fields are present. Prohibited if the subject:organizationName field is absent.	If present, the subject:localityName field MUST contain the Subject's locality information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the localityName field MAY contain the Subject 's locality and/or state or province information as verified under Section 11.2.

Relative Distinguished Name Type	Required/Optional	Contents
stateOrProvinceName (OID: 2.5.4.8)	Required if the subject:organizationName field is present and subject:localityName field is absent. Optional if subject:organizationName and subject:localityName fields are present. Prohibited if the subject:organizationName field is absent.	If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 11.2. If the subject:countryName field specifies the ISO 3166-1 user-assigned code of XX in accordance with Section 9.2.5, the subject:stateOrProvinceName field MAY contain the full name of the Subject's country information as verified under Section 11.2.5.
postalCode (OID: 2.5.4.17)	Optional if the subject:organizationName field is present. Prohibited if the subject:organizationName field is absent.	If present, the subject:postalCode field MUST contain the Subject's zip or postal information as verified under Section 11.2
countryName (OID: 2.5.4.6)	Required if the subject:organizationName field is present. Optional if the subject:organizationName field is absent.	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 11.2. If the subject:organizationName field is absent, the subject:countryName field MAY contain the two-letter ISO 3166-1 country code associated with the Subject as verified in accordance with Section 11.2.5. If a Country is not represented by an official ISO 3166-1 country code, the CA 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.

Relative Distinguished Name Type	Required/Optional	Contents
organizationalUnitName	Optional.	The CA SHALL implement 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 Section 11.2 and the Certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with Section 11.2.

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

7.1.4.3 Subject Alternative Names for Standard Server Authentication certificates

The Subject Alternative Name Extension MUST contain at least one entry. Each entry MUST be either a dNSName containing the Fully-Qualified Domain Name or an iPAddress containing the IP address of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name 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.

As of the Effective Date of these Requirements, prior to the issuance of a Certificate with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name, the CA SHALL notify the Applicant that the use of such Certificates has been deprecated by the CA / Browser Forum and that the practice will be eliminated by October 2016. Also as of the Effective Date, the CA SHALL NOT issue a certificate with an Expiry Date later than 1 November 2015 with a subjectAlternativeName extension or Subject commonName field containing a Reserved IP Address or Internal Name. Effective 1 October 2016, CAs SHALL revoke all unexpired Certificates whose subjectAlternativeName extension or Subject commonName field contains a Reserved IP Address or Internal Name.

7.1.4.4 Subject Information for Extended Validation Server Authentication certificates

Subject to the requirements of this Certificate Policy, the EV Certificate and certificates issued to Subordinate CAs that are not controlled by the same entity as the CA MUST include the following information about the Subject organization in the fields listed:

Relative Distinguished Name Type	Required/ Optional	Contents
organizationName (OID 2.5.4.10)	Required	This field MUST contain the Subject's full legal organization name as listed in the official records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration or as otherwise verified by the CA as provided herein. A CA MAY abbreviate the organization prefixes or suffixes in the organization name, e.g., if the official record shows "Company Name Incorporated" the CA MAY include "Company Name, Inc." When abbreviating a Subject's full legal name as allowed by this subsection, the CA MUST use abbreviations that are not misleading in the Jurisdiction of Incorporation or Registration. In addition, an assumed name or DBA name used by the Subject MAY be included at the beginning of this field, provided that it is followed by the full legal organization name in parenthesis. If the combination of names or the organization name by itself exceeds 64 characters, the CA MAY abbreviate parts of the organization name, and/or omit non-material words in the organization name in such a way that the text in this field does not exceed the 64-character limit; provided that the CA checks this field in accordance with EV Guidelines section 11.12.1 and a Relying Party will not be misled into thinking that they are dealing with a different organization. In cases where this is not possible, the CA MUST NOT issue the EV Certificate.
commonName (OID: 2.5.4.3)	Deprecated (Discouraged, but not prohibited)	If present, this field MUST contain a single Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV Certificates.
businessCategory (OID: 2.5.4.15)	Required	This field MUST contain one of the following strings: " Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity" depending upon whether the Subject qualifies under the terms of EV Guidelines Section 8.5.2, 8.5.3, 8.5.4 or 8.5.5 of this Certificate Policy, respectively.
jurisdictionLocalityName (OID: 1.3.6.1.4.1.311.60.2.1.1)	Required/ Optional	See jurisdictionCountryName
jurisdictionStateOrProvinceName (OID: 1.3.6.1.4.1.311.60.2.1.2)	Required/ Optional	See jurisdictionCountryName

Relative Distinguished Name Type	Required/ Optional	Contents
jurisdictionCountryName (OID: 1.3.6.1.4.1.311.60.2.1.3)	Required	These fields MUST NOT contain information that is not relevant to the level of the Incorporating Agency or Registration Agency. For example, the Jurisdiction of Incorporation for an Incorporating Agency or Jurisdiction of Registration for a Registration Agency that operates at the country level MUST include the country information but MUST NOT include the state or province or locality information. Similarly, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the state or province level MUST include both country and state or province information, but MUST NOT include locality information. And, the jurisdiction for the applicable Incorporating Agency or Registration Agency at the locality level MUST include the country and state or province information, where the state or province regulates the registration of the entities at the locality level, as well as the locality information. Country information MUST be specified using the applicable ISO country code. State or province or locality information (where applicable) for the Subject's Jurisdiction of Incorporation or Registration MUST be specified using the full name of the applicable jurisdiction

Relative Distinguished Name Type	Required/ Optional	Contents
serialNumber (OID: 2.5.4.5)	Required	For Private Organizations, this field MUST contain the Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate. If the Jurisdiction of Incorporation or Registration does not provide a Registration Number, then the date of Incorporation or Registration SHALL be entered into this field in any one of the common date formats. For Government Entities that do not have a Registration Number or readily verifiable date of creation, the CA SHALL enter appropriate language to indicate that the Subject is a Government Entity. For Business Entities, the Registration Number that was received by the Business Entity upon government registration SHALL be entered in this field. For those Business Entities that register with an Incorporating Agency or Registration Agency in a jurisdiction that does not issue numbers pursuant to government registration, the date of the registration SHALL be entered into this field in any one of the common date formats.
streetAddress (OID: 2.5.4.9)	Optional	This field MUST contain the address of the physical location of the Subject's Place of Business.
localityName (OID: 2.5.4.7)	Required	This field MUST contain the address of the physical location of the Subject's Place of Business.
stateOrProvinceName (OID: 2.5.4.8)	Required where applicable	This field MUST contain the address of the physical location of the Subject's Place of Business, if the country has principal subdivisions.
countryName (OID: 2.5.4.6)	Required	This field MUST contain the address of the physical location of the Subject's Place of Business.
postalCode (OID: 2.5.4.17)	Optional	This field MUST contain the address of the physical location of the Subject's Place of Business.

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the CA. CAs SHALL NOT include Fully-Qualified Domain Names in Subject attributes except as specified in EV Guidelines Section 9.2.1 and SHALL NOT include any Subject Organization Information except as specified in EV Guidelines Section 9.2. Optional subfields within the Subject field MUST either contain information verified by the CA or MUST be left empty. Metadata such as '.', '-', and ' ' characters, and/ or any other indication that the field is empty, absent or incomplete, MUST not be used.

7.1.4.5 Subject Alternative Names for Extended Validation Server Authentication certificates

This extension MUST contain one or more host Domain Name(s) owned or controlled by the Subject and to be associated with the Subject's server. Such server MAY be owned and operated by the Subject or another entity (e.g., a hosting service). Wildcard certificates are not allowed for EV Certificates.

7.1.4.6 Subject Information for Extended Validation Code Signing certificates

EV Code Signing Objects issued to Subscribers MUST include the following information about the Subject organization in the fields listed:

Relative Distinguished Name Type	**Contents**
Subject Organization Name	As specified in Section 9.2.1 of the EV Guidelines.
Subject Common Name	Deprecated. If present, this field MUST NOT contain a Domain Name.
Subject Business Category	As specified in Section 9.2.4 of the EV Guidelines.
Subject Jurisdiction of Incorporation or Registration	As specified in Section 9.2.5 of the EV Guidelines.
Subject Registration Number	As specified in Section 9.2.6 of the EV Guidelines.
Subject Physical Address of Place of Business	As specified in Section 9.2.7 of the EV Guidelines.

All other optional attributes, when present within the subject field, MUST contain information that has been verified by the Issuer. Optional subfields within the Subject field MUST either contain information verified by the Issuer or MUST be left empty. Metadata such as '.', '-', and ' ' characters, and/or any other indication that the field is empty, absent or incomplete, MUST not be used.

7.1.5 Name constraints

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

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then the Subordinate CA Certificate MUST include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and DirectoryName as follows:- (a) For each dNSName in permittedSubtrees, the CA MUST confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of section 3.2.2.4. (b) For each iPAddress range in permittedSubtrees, the CA MUST confirm that the Applicant has been assigned the iPAddress range or has been authorized by the assigner to act on the assignee's behalf. (c) For each DirectoryName in permittedSubtrees the CA MUST confirm the Applicants and/or Subsidiary's Organizational name and location such that end entity certificates issued from the subordinate CA Certificate will be in compliancy with section 7.1.2.4 and 7.1.4.2.5.

If the Subordinate CA Certificate is not allowed to issue certificates with an iPAddress, then the Subordinate CA Certificate MUST specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate MUST include within excludedSubtrees an iPAddress GeneralName of 8 zero octets (covering the IPv4 address range of 0.0.0.0/0). The Subordinate CA Certificate MUST also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0). Otherwise, the Subordinate CA Certificate MUST include at least one iPAddress in permittedSubtrees.

A decoded example for issuance to the domain and sub domains of example.com by organization :- Example LLC, Boston, Massachusetts, US would be:- X509v3 Name Constraints: Permitted: DNS:example.com DirName: C=US, ST=MA, L=Boston, O=Example LLC Excluded: IP:0.0.0.0/0.0.0.0 IP: 0:0:0:0:0:0:0:0/0:0:0:0:0:0:0:0

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

7.1.6 Certificate policy object identifier

As specified in Section 9.3 of the EV Guidelines.

7.1.6.1. Reserved Certificate Policy Identifiers

The following Certificate Policy identifiers are reserved for use by CAs as an optional means of asserting compliance with these Requirements as follows:

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) domain-validated(1)} (2.23.140.1.2.1), if the Certificate complies with these Requirements but lacks Subject Identity Information that is verified in accordance with Section 3.2.2.1.

If the Certificate asserts the policy identifier of 2.23.140.1.2.1, then it MUST NOT include organizationName, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.

{joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) subject-identity-validated(2)} (2.23.140.1.2.2), if the Certificate complies with these Requirements and includes Subject Identity Information that is verified in accordance with Section 3.2.2.1.

If the Certificate asserts the policy identifier of 2.23.140.1.2.2, then it MUST also include organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.

Each EV Certificate issued by the CA to a Subscriber MUST contain a policy identifier defined by the CA in the certificate's certificatePolicies extension that: (i) indicates which CA policy statement relates to that Certificate, (ii) asserts the CA's adherence to and compliance with this Certificate Policy, and (iii), by pre-agreement with the Application Software Supplier, marks the Certificate as being an EV Certificate.

7.1.6.2. Root CA Certificates

A Root CA Certificate SHOULD NOT contain the certificatePolicies extension.

The Application Software Supplier identifies Root CAs that are approved to issue EV Certificates by storing EV policy identifiers in metadata associated with Root CA Certificates.

7.1.6.3 Subordinate CA Certificates

A Certificate issued after the Effective Date to a Subordinate CA that is not an Affiliate of the Issuing CA: 1. MUST include one or more explicit policy identifiers that indicates the Subordinate CA's adherence to and compliance with these Requirements (i.e. either the CA/Browser Forum reserved identifiers or identifiers defined by the CA in its Certificate Policy and/or Certification Practice Statement) and 2. MUST NOT contain the "anyPolicy" identifier (2.5.29.32.0). A Certificate issued after the Effective Date to a Subordinate CA that is an affiliate of the Issuing CA: 1. MAY include the CA/Browser Forum reserved identifiers or an identifier defined by the CA in its Certificate Policy and/or Certification Practice Statement to indicate the Subordinate CA's compliance with these Requirements and 2. MAY contain the "anyPolicy" identifier (2.5.29.32.0) in place of an explicit policy identifier. A Subordinate CA SHALL represent, in its Certificate Policy and/or Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with these Requirements are issued and managed in accordance with these Requirements.

1. Certificates issued to Subordinate CAs that are not controlled by the issuing CA MUST contain one or more policy identifiers defined by the issuing CA that explicitly identify the EV Policies that are implemented by the Subordinate CA.
2. Certificates issued to Subordinate CAs that are controlled by the Root CA MAY contain the special anyPolicy identifier (OID: 2.5.29.32.0).

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 its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with these Requirements.

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 this Certificate Policy. Each CA SHALL document in its Certificate Policy or Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with this Certificate Policy.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

No stipulation.

7.2.2 CRL and CRL entry extensions

No stipulation.

7.3 OCSP profile

7.3.1 Version number(s)

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The CA SHALL at all times:

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

8.1 Frequency or circumstances of assessment

Certificates that are capable of being used to issue new certificates MUST either be Technically Constrained in line with section 7.1.5 and audited in line with section 8.7 only, or Unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new certificates if it contains an X.509v3 basicConstraints extension, with the cA boolean set to true and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the CA issues Certificates SHALL be divided into an unbroken sequence of audit periods. An audit period MUST NOT exceed one year in duration.

If the CA has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.1, then no pre-issuance readiness assessment is necessary.

If the CA does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.1, then, before issuing Publicly-Trusted Certificates, the CA SHALL successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.1. The point-in-time readiness assessment SHALL be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted Certificates and SHALL be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted Certificate.

CAs issuing EV Certificates MUST undergo an annual audit that meets the criteria of 8.4.

If the CA has a currently valid WebTrust Seal of Assurance for CAs, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against the WebTrust EV Program.

If the CA has a currently valid ETSI 102 042 audit, then, before issuing EV Certificates, the CA and its Root CA MUST successfully complete a point-in-time readiness assessment audit against ETSI TS 102 042.

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

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

Issuers MUST undergo an annual audit that meets the criteria of section 8.4.

Issuers that are not already issuing EV Certificates must obtain a pre-issuance readiness audit under Section 17.4 of the EV Guidelines.

8.2 Identity/qualifications of assessor

The CA's audit SHALL be performed by a Qualified Auditor. A Qualified Auditor means a natural person, Legal Entity, or group of natural persons or Legal Entities that collectively possess the following qualifications and skills: 1. Independence from the subject of the audit; 2. The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.1); 3. Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function; 4. (For audits conducted in accordance with any one of the ETSI standards) accredited in accordance with ETSI TS 119 403, or accredited to conduct such audits under an equivalent national scheme, or accredited by a national accreditation body in line with ISO 27006 to carry out ISO 27001 audits; 5. (For audits conducted in accordance with the WebTrust standard) licensed by WebTrust; 6. Bound by law, government regulation, or professional code of ethics; and 7. Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors &

Omissions insurance with policy limits of at least one million US dollars in coverage

8.3 Assessor's relationship to assessed entity

8.4 Topics covered by assessment

The CA SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust for Certification Authorities v2.0;
2. A national scheme that audits conformance to ETSI TS 102 042;
3. A scheme that audits conformance to ISO 21188:2006; or
4. If a Government CA is required by its Certificate Policy to use a different internal audit scheme, it MAY use such scheme provided that the audit either (a) encompasses all requirements of one of the above schemes or (b) consists of comparable criteria that are available for public review.

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

The audit MUST be conducted by a Qualified Auditor, as specified in Section 8.3.

If a Delegated Third Party is not currently audited in accordance with Section 8 and is not an Enterprise RA, then prior to certificate issuance the CA SHALL ensure that the domain control validation process required under Section 3.2.2.4 or IP address verification under 3.2.2.5 has been properly performed by the Delegated Third Party by either (1) using an out-of-band mechanism involving at least one human who is acting either on behalf of the CA or on behalf of the Delegated Third Party to confirm the authenticity of the certificate request or the information supporting the certificate request or (2) performing the domain control validation process itself.

If the CA is not using one of the above procedures and the Delegated Third Party is not an Enterprise RA, then the CA SHALL obtain an audit report, issued under the auditing standards that underlie the accepted audit schemes found in Section 8.1, that provides an opinion whether the Delegated Third Party's performance complies with either the Delegated Third Party's practice statement or the CA's Certificate Policy and/or Certification Practice Statement. If the opinion is that the Delegated Third Party does not comply, then the CA SHALL not allow the Delegated Third Party to continue performing delegated functions.

The audit period for the Delegated Third Party SHALL NOT exceed one year (ideally aligned with the CA's audit). However, if the CA or Delegated Third Party is under the operation, control, or supervision of a Government Entity and the audit scheme is completed over multiple years, then the annual audit MUST cover at least the core controls that are required to be audited annually by such scheme plus that portion of all non-core controls that are allowed to be conducted less frequently, but in no case may any non-core control be audited less often than once every three years.

A CA issuing EV Certificates SHALL undergo an audit in accordance with one of the following schemes:

1. WebTrust Program for CAs audit and WebTrust EV Program audit, or
2. ETSI TS 102 042 audit.

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

EV audits MUST cover all CA obligations under this Certificate Policy regardless of whether they are performed directly by the CA or delegated to an RA or subcontractor.

An Issuer issuing EV Code Signing Objects SHALL undergo an audit in accordance with one of the following schemes: (i) WebTrust Program for CAs audit and WebTrust EV Program audit, or (ii) ETSI TS 102 042 v2.1.1 audit. If the Issuer is a Government Entity, an audit of the Issuer by the appropriate internal government auditing agency is acceptable in lieu of the audits specified above, provided that such internal government auditing agency publicly certifies in writing that its audit addresses the criteria specified in one of the above audit schemes and certifies that the government Issuer has successfully passed the audit. EV audits MUST cover all Issuer obligations under this Certificate Policy regardless of whether they are performed directly by the Issuer, an RA, or subcontractor.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

The Audit Report SHALL state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in Section 7.1.6.1. The CA SHALL make the Audit Report publicly available. The CA is not required to make publicly available any general audit findings that do not impact the overall audit opinion. For both government and commercial CAs, the CA SHOULD make its Audit Report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, and if so requested by an Application Software Supplier, the CA SHALL provide an explanatory letter signed by the Qualified Auditor.

CAs SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the CA MUST provide an explanatory letter signed by its auditor.

Issuers SHOULD make its audit report publicly available no later than three months after the end of the audit period. If there is a delay greater than three months and if so requested by an Application Software Supplier, the Issuer MUST provide an explanatory letter signed by its auditor.

8.7 Self-Audits

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

The CA SHALL internally audit each Delegated Third Party's compliance with these Requirements on an annual basis.

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

During the period in which it issues EV Certificates, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.13 of this Certificate Policy is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Certificates it has issued in the period beginning immediately after the last sample was taken.

Issuers must abide by the self audit requirements of the EV Guidelines. During the period in which it issues EV Code Signing Certificates, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least three percent of the EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken. For all EV Code Signing Certificates where the Final Cross-Correlation and Due Diligence requirements of Section 11.12 of this Certificate Policy is performed by an RA, the CA MUST strictly control its service quality by performing ongoing self audits against a randomly selected sample of at least six percent of the EV Code Signing Certificates it has issued in the period beginning immediately after the last sample was taken.

9 OTHER BUSINESS AND LEGAL MATTERS

The CA must maintain controls to provide reasonable assurance that it conforms with the relevant legal, regulatory and contractual requirements.

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No stipulation.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

9.2.1 Insurance coverage

Each CA SHALL maintain the following insurance related to their respective performance and obligations under this Certificate Policy:

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

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

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

9.2.2 Other assets

No stipulation.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a Certificate, the CA makes the certificate warranties listed herein to the following Certificate Beneficiaries:

1. The Subscriber that is a party to the Subscriber or Terms of Use Agreement for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate. The CA represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the CA has complied with these Requirements and its Certificate Policy and/or Certification Practice Statement in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following: 1. Right to Use Domain Name or IP Address: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement; 2. Authorization for Certificate: That, at the time of issuance, the CA (i) implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement; 3. Accuracy of Information: That, at the time of issuance, the CA (i) implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute); (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement; 4. No Misleading Information: That, at the time of issuance, the CA (i) implemented a procedure for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement; 5. Identity of Applicant: That, if the Certificate contains Subject Identity Information, the CA (i) implemented a procedure to verify the identity of the Applicant in accordance with Sections 3.2 and 11.2; (ii) followed the procedure when issuing the Certificate; and (iii) accurately described the procedure in the CA's Certificate Policy and/or Certification Practice Statement; 6. Subscriber Agreement: That, if the CA and Subscriber are not Affiliated, the Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the CA and Subscriber are Affiliated, the Applicant Representative acknowledged and accepted the Terms of Use; 7. Status: That the CA maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (valid or revoked) of all unexpired Certificates; and 8. Revocation: That the CA will revoke the Certificate for any of the reasons specified in these Requirements.

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

For Extended Validation certificates, the EV Certificate Warranties specifically include, but are not limited to, the following: 1. Legal Existence: The CA has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration; 2. Identity: The CA has confirmed that, as of the date the EV Certificate was issued, the legal name of the Subject named in the EV Certificate matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business; 3. Right to Use Domain Name: The CA has taken all steps reasonably necessary to verify that, as of the date the EV Certificate was issued, the Subject named in the EV Certificate has the right to use all the Domain Name(s) listed in the EV Certificate; 4. Authorization for EV Certificate: The CA has taken all steps reasonably necessary to verify that the Subject named in the EV Certificate has authorized the issuance of the EV Certificate; 5. Accuracy of Information:

The CA has taken all steps reasonably necessary to verify that all of the other information in the EV Certificate is accurate, as of the date the EV Certificate was issued; 6. Subscriber Agreement: The Subject named in the EV Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA that satisfies the requirements of this Certificate Policy or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use; 7. Status: The CA will follow the requirements of this Certificate Policy and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Certificate as Valid or revoked; and 8. Revocation: The CA will follow the requirements of this Certificate Policy and revoke the EV Certificate for any of the revocation reasons specified in this Certificate Policy.

When a CA issues an EV Code Signing Certificate, the CA and its Root CA represents and warrants to the Certificate Beneficiaries listed in Section 7.1.1 of the Baseline Requirements, during the period when the EV Code Signing Certificate is Valid, that the CA has followed the requirements of this Certificate Policy and its EV Policies in issuing and managing the EV Code Signing Certificate and in verifying the accuracy of the information contained in the EV Code Signing Certificate. Similarly, when a Signing Authority provides an EV Signature, the Signing Authority represents and warrants to the Certificate Beneficiaries listed in Section 7.1.1 of the Baseline Requirements, during the period when the EV Signature is Valid, that the CA has followed the requirements in providing the EV Signature to the Subscriber. These warranties specifically include, but are not limited to, the following: (A) Legal Existence: The Issuer has confirmed with the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration that, as of the date the EV Code Signing Object was issued, the Subject of the EV Code Signing Object legally exists as a valid organization or entity in the Jurisdiction of Incorporation or Registration; (B) Identity: The Issuer has confirmed that, as of the date the EV Code Signing Object was issued, the legal name of the Subject named in the EV Code Signing Object matches the name on the official government records of the Incorporating or Registration Agency in the Subject's Jurisdiction of Incorporation or Registration, and if an assumed name is also included, that the assumed name is properly registered by the Subject in the jurisdiction of its Place of Business; 6 (C) Authorization for EV Code Signing Certificate: The Issuer has taken all steps reasonably necessary to verify that the Subject of the EV Code Signing Object authorized the issuance of the EV Code Signing Object; (D) Accuracy of Information: The Issuer has taken all steps reasonably necessary to verify that all of the other information in the EV Code Signing Object is accurate, as of the date of issuance; (E) Subscriber Agreement: The Subject of the EV Code Signing Object has entered into a legally valid and enforceable Subscriber Agreement with the Issuer that satisfies the requirements of this Certificate Policy or, if they are affiliated, the Applicant Representative has acknowledged and accepted the Terms of Use; (F) Status: The Issuer will follow the requirements of this Certificate Policy and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the EV Code Signing Object as Valid or revoked; and (G) Revocation: The Issuer will follow the requirements of this Certificate Policy and revoke the EV Code Signing Object for any of the revocation reasons specified in this Certificate Policy.

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

The CA maintains controls to provide reasonable assurance that requirements for protection of subscriber keys are communicated to subscribers.

The CA SHALL require, as part of the Subscriber or Terms of Use Agreement, that the Applicant make the commitments and warranties in this section for the benefit of the CA and the Certificate Beneficiaries.

Prior to the issuance of a Certificate, the CA SHALL obtain, for the express benefit of the CA and the Certificate Beneficiaries, either: 1. The Applicant's agreement to the Subscriber Agreement with the CA, or 2. The Applicant's agreement to the Terms of Use agreement.

The CA SHALL implement a process to ensure that each Subscriber or Terms of Use 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. The CA MAY use an electronic or "click-through" Agreement provided that the CA has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each certificate request, or a single Agreement MAY be used to cover multiple future certificate requests and the resulting Certificates, so long as each Certificate that the CA issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

The Subscriber or Terms of Use Agreement MUST contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties: 1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA; 2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token); 3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy; 4. Use of Certificate: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber or Terms of Use Agreement; 5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: (a) any information in the Certificate is, or becomes, incorrect or inaccurate, or (b) there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate; 6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise. 7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period. 8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware.

Prior to issuing an EV Code Signing Object, the Issuer SHALL obtain, for the express benefit of the Issuer and the Certificate Beneficiaries, either:

1. The Applicant's agreement to the Subscriber Agreement with the Issuer, or
2. The Applicant's agreement to the Terms of Use agreement. The Issuer SHALL implement a process to ensure that each Subscriber or Terms of Use Agreement is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the EV Code Signing Object to be issued pursuant to the certificate request. The Issuer MAY use an electronic or "click-through" Agreement provided that the

Issuer has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each EV Code Signing Object request, or a single Agreement MAY be used to cover multiple future EV Code Signing Object requests and the resulting objects, so long as each EV Code Signing Object that the Issuer issues to the Applicant is clearly covered by that Subscriber or Terms of Use Agreement.

CAs MUST impose the following obligations and warranties on each Applicant (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) using a Subscriber or Terms of Use Agreement: 1. Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the CA, both in the certificate request and as otherwise requested by the CA in connection with the issuance of the Certificate(s) to be supplied by the CA; 2. Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to maintain sole control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token); 3. Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy; 4. Use of the Certificate: An obligation and warranty to not knowingly sign software that contains Suspect Code and use the EV Code Signing Certificate as follows: a. only to sign code that complies with the requirements set forth in this Certificate Policy; b. solely in compliance with all applicable laws; c. solely for authorized company business; and d. solely in accordance with the Subscriber Agreement; 5. Reporting and Revocation: An obligation and warranty to promptly cease using a Certificate and its associated Private Key, and promptly request the CA to revoke the Certificate, in the event that: a. there is evidence that the certificate was used to sign suspect code; b. any information in the Certificate is, or becomes, incorrect or inaccurate; or c. there is any actual or suspected misuse or compromise of either the key activation data or the Subscriber's Private Key associated with the Public Key included in the Certificate; 6. Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise. 7. Responsiveness: An obligation to respond to the CA's instructions concerning Key Compromise or Certificate misuse within a specified time period. 8. Acknowledgment and Acceptance: An acknowledgment and acceptance that the CA is entitled to revoke the certificate immediately if the Applicant were to violate the terms of the Subscriber or Terms of Use Forum Guideline Agreement or if the CA discovers that the Certificate is being used to enable criminal activities such as phishing attacks, fraud, or the distribution of malware. If a Signing Authority becomes aware (by whatever means) that it has signed code that contains malicious software or a serious vulnerability, then it MUST immediately inform the issuing CA. If a Signing Authority's private key, or private key activation data, is compromised or believed to be compromised, the Signing Authority MUST contact the issuing CA immediately and request that the certificate be revoked Signing Authorities must obtain a Subscriber or Terms of Use Agreement with its customer that contains the following obligations and warranties: 1. To use the EV Signature solely in compliance with the requirements set forth herein and the applicable EV Guidelines; 2. To use the EV Signature solely in compliance with all applicable laws; 3. To use the EV Signature solely for authorized company business; 4. To use the EV Signature solely in accordance with the Subscriber or Terms of Use Agreement; 5. To not knowingly submit software for signature that contains Suspect Code; 6. To inform the Signing Authority if it is discovered (by whatever means) that code submitted to the Signing Authority for signature contains malware or a serious vulnerability.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of liability

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

If the CA has issued and managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY disclaim liability to the Certificate Beneficiaries or any other third parties for any losses suffered as a result of use or reliance on such Certificate beyond those specified in the CA's Certificate Policy and/or Certification Practice Statement. If the CA has not issued or managed the Certificate in compliance with these Requirements and its Certificate Policy and/or Certification Practice Statement, the CA MAY seek to limit its liability to the Subscriber and to Relying Parties, regardless of the cause of action or legal theory involved, for any and all claims, losses or damages suffered as a result of the use or reliance on such Certificate by any appropriate means that the CA desires. If the CA chooses to limit its liability for Certificates that are not issued or managed in compliance with these Requirements or its Certificate Policy and/or Certification Practice Statement, then the CA SHALL include the limitations on liability in the CA's Certificate Policy and/or Certification Practice Statement.

A CA MAY NOT limit its liability to Subscribers or Relying Parties for legally recognized and provable claims to a monetary amount less than two thousand US dollars per Subscriber or Relying Party per EV Certificate.

9.9 Indemnities

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the CA understands and acknowledges that the Application Software Suppliers who have a Root Certificate distribution agreement in place with the Root CA do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the CA is a government entity, the CA SHALL defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the CA, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy: (1) a Certificate that has expired, or (2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and termination

9.10.1 Term

No stipulation.

9.10.2 Termination

No stipulation.

9.10.3 Effect of termination and survival

No stipulation.

9.11 Individual notices and communications with participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for amendment

No stipulation.

9.12.2 Notification mechanism and period

No stipulation.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

No stipulation.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If a court or government body with jurisdiction over the activities covered by these Requirements determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify the CA / Browser Forum of the facts, circumstances, and law(s) involved, so that the CA/Browser Forum may revise these Requirements accordingly.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

---

1. 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/ (http://publicsuffix.org/) (PSL), and to retrieve a fresh copy regularly. If using the PSL, a CA SHOULD consult the "ICANN DOMAINS" section only, not the "PRIVATE DOMAINS" section. The PSL is updated regularly to contain new gTLDs delegated by ICANN, which are listed in the "ICANN DOMAINS" section. A CA is not prohibited from issuing a Wildcard Certificate to the Registrant of an entire gTLD, provided that control of the entire namespace is demonstrated in an appropriate way.

No stipulation.