Federal Public Trust Device Certificate Policy

DRAFT

Version 0.1

September 2017

Table of Contents

1. INTRODUCTION

1.1 Overview

This Certificate Policy (CP) outlines the policy and requirements for the U.S. Federal Public Key Infrastructure, and the issuance and management of U.S. Federal Publicly Trusted Device Certificates. The certificates under this policy are for identifying and authenticating government services. This policy incorporates Certificate Transparency as a key component in promoting publicly accessible and accountable services.

This document serves two purposes:

- to specify the Federal Public Device PKI Certificate Policy and requirements, and
- to provide requirements for what each Certification Authority must address in its Certification Practices Statement

This policy is for a hierarchical Public Key Infrastructure restricted to services operated by or on behalf of the U.S. Government and U.S. Federal entities. The hierarchical PKI is referenced as the **Federal Public Device PKI** in this document.

This policy and requirements are applicable to all Certification Authorities within a chain of trust under the **US Federal Device Root CA**. The requirements are to be flowed down from the Root Certification Authority through all Subordinate Certification Authorities.

The Federal Public Device PKI conforms to the Version 1.4.9 of the guidelines adopted by the Certification Authority/Browser Forum ("CA/Browser Forum") when issuing publicly trusted certificates, including the Baseline Requirements for the Issuance and Management of Publicly Trusted Certificates ("Baseline Requirements"). This document is based on the CA/Browser Forum Baseline Requirements, which is licensed under the Creative Commons Attribution 4.0 International License. All additions and modifications made to create this document are in the public domain as works of the U.S. Government, and copyright and related rights in the work are waived.

Additional documents related to the Federal Public Device PKI, such as Certification Practices Statements, Audits, and Subscriber Agreement(s) can be found at <INSERT URL HERE>.

In accordance with RFC 3647, this CP includes all nine sections of the RFC 3647 framework and an additional addendum with the certificate profiles.

The terms and provisions of this certificate policy shall be interpreted under and governed by applicable Federal law.

The following Certification Authorities are covered under this CP:

CA Type	Distinguished Name	Key Pair Type and Parameters	SHA-256 Key Fingerprint	Validity Period
Root CA	<INSERT DN>	<INSERT RSA>	<INSERT SHA-256 FINGERPRINT>	<INSERT VALIDITY PERIOD>
Subordinate CA	<INSERT DN>	<INSERT RSA>	<INSERT SHA-256 FINGERPRINT>	<INSERT VALIDITY PERIOD>

1.2 Document name and identification

This is the Federal Public Device PKI Certificate Policy.

The following Certificate Policy identifiers are reserved for use by CAs as a means of asserting compliance with this CP:

OID Arc	Owner	OID	Description
2.16.840.1.101.3.2.1	NIST Computer Security Objects Register (CSOR), Public Key Infrastructure (PKI) Objects Registration	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) certificate-policies(1) } (2.16.840.1.101.3.2.1)	TBD
2.16.840.1.101.3.2.1	NIST Computer Security Objects Register (CSOR), Public Key Infrastructure (PKI) Objects Registration	{joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) certificate-policies(1) } (2.16.840.1.101.3.2.1)	TBD

1.2.1. Revisions

Ver.	Change Proposal	Description	Adopted	Effective*
1.0.0	<TBD>	Version 1.0 of the Certificate Policy Adopted	<TBD>	<TBD>

* Effective Date and Additionally Relevant Compliance Date(s)

1.2.2. Relevant Dates

Compliance	Section(s)	Summary Description (See Full Text for Details)
yyyy-mm-dd	<TBD>	Description

1.3 PKI Participants

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is a sub-council comprised of U.S. Federal Government Agency representatives and is chartered by the U.S. Federal CIO Council. The FPKIPA manages this policy and represents the interests of the U.S. Federal CIOs and CISOs.

1.3.1 Certification Authorities

The Certification Authorities operated under this policy provide services to U.S. Federal Government entities which may be part of the Executive Branch, Legislative Branch and Judicial Branch of the Federal Government. The services are not provided to the general public, commercial entities, U.S. State, Local, Territorial, Native Sovereign Nations, or international government entities.

Certification Authority (CA) is defined in Section 1.6.

1.3.2 Registration Authorities

This Certificate Policy is focused on promoting automation, improving efficiencies, supporting operational security, and establishing trust in the U.S. Government and the digital services operated by or on behalf of U.S. Federal Government entities. The widespread adoption of practices and protocols to support automation in certificate management have been foundational to increases in the deployment of secure protocols for webservices.

While this policy promotes automation for the Certification Authorities, there still exists a need to allow a delegation of responsibility to U.S. Federal Government entities that form part of the U.S. Federal Government enterprise.

This policy allows for persons who may not be affiliated with the same organizational unit that is operating the Certificate Authority to assist in the certificate application process and be designated as Enterprise Registration Authorities as a role. Registration Authority system functions shall be the responsibility of the Certificate Authority.

A CA MAY designate an Enterprise Registration Authority (RA) to verify certificate requests from the Enterprise RA's affiliated U.S. Federal Government entity. 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(s) as registered in the .GOV (DotGov) and .MIL (DotMil) gTLDs Domain Name Registrars.
2. The CA SHOULD confirm that the requested Fully-Qualified Domain Name(s) are not within any Domain Namespace(s) for any U.S. State, Local, Territorial, Native Sovereign Nations, or any other entities identified as a *Non-Federal Agency* in the DotGov Domain Name Registrar per United States Code (U.S.C.) 41 CFR Part 102-173.

The CA SHALL impose these limitations through an agreement with the Authorizing Authority of the Domain Name as defined under United States Code (U.S.C.) 41 CFR Part 102-173. The CA SHALL monitor compliance by the Enterprise RA and institute technical controls. The CA SHOULD use both audits and analytics based methods such as monitoring of Certificate Transparency Log(s) and services to ensure compliance.

Delegated Third Parties are not allowed under this policy.

1.3.3 Subscribers

As defined in Section 1.6.1.

1.3.4 Relying Parties

"Relying Party" and "Application Software Supplier" are defined in Section 1.6.1.

Relying Parties should verify the validity of certificates via revocation services provided for all certificates prior to relying on certificates. Certificate Revocation List (CRL) and On-line Certificate Status Protocol (OCSP) service location information is provided within certificates.

1.3.5 Other Participants

Not applicable.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

This Certificate Policy (CP) and requirements for U.S. Federal Government is limited to Publicly Trusted Device Certificates used for identifying and authenticating devices and services. Certificates may be used for all legal authentication and encryption purposes.

1.4.2 Prohibited Certificate Uses

Certificates may not be used where prohibited by law.

Certificates for identifying natural persons are not allowed under this policy and the Federal Public Device PKI, including but not limited to identity certificates used to identify natural persons for digital signatures, S/MIME, client authentication, and encryption. CAs may not issue Subscriber certificates for natural persons or enter into any cross-certification with any CAs that issue certificates used to identify and authenticate natural persons.

1.5 Policy administration

The Federal Public Key Infrastructure Policy Authority (FPKIPA) manages this policy and represents the interests of the U.S. Federal CIOs and CISOs.

1.5.1 Organization Administering the Document

The Federal Public Key Infrastructure Policy Authority (FPKIPA) is responsible for:

- Maintaining this CP, and
- Approving the CPS for each CA that issues certificates under this policy, and
- Approving the compliance audit report for each CA issuing certificates under this policy, and
- Ensuring continued conformance of each CA that issues certificates under this policy with applicable requirements as a condition for allowing continued participation, and
- Ensuring compliance with CA/Browser Forum Baseline Requirements, and

- Ensuring compliance with any trust store requirements and any browser requirements that the Federal Device Root pursues or has inclusion in.

1.5.2 Contact Person

Contact information for the Federal Public Key Infrastructure Policy Authority is fpki@gsa.gov.

1.5.3 Person Determining CPS suitability for the policy

Federal Public Key Infrastructure Policy Authority

1.5.4 CPS approval procedures

A CPS shall be submitted and approved by the Federal Public Key Infrastructure Policy Authority.

Prior to submitting a CPS, the CA shall commission a compliance analysis study culminating in a written report that provides a summary of areas in which the CPS may not or does not comply with this CP. The compliance analysis shall be performed by an independent party. The CA shall resolve these discrepancies prior to submitting the CPS to the Policy Authority. The CA must have an approved CPS and meet all CP and CPS requirements prior to commencing operations.

1.6 Definitions and Acronyms

1.6.1 Definitions

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.

Air-Gapped: Certificate Systems or components that are physcially and logically disconnected from the public internet.

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 the Terms of Use on behalf of the Applicant when the Applicant is an Affiliate of the CA or is the CA.

Application Software Supplier: A supplier of Internet browser software or other relying-party application software that displays or uses Certificates and incorporates Root Certificates.

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

Audit Period: In a period-of-time audit, the period between the first day (start) and the last day of operations (end) covered by the auditors in their engagement. (This is not the same as the period of time when the auditors are on-site at the CA.) The coverage rules and maximum length of audit periods are defined in section 8.1.

Audit Report: A report from a Qualified Auditor stating the Qualified Auditor's opinion on whether an entity's processes and controls comply with the mandatory provisions of these Requirements.

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

Authorized Port: One of the following ports: 80 (http), 443 (http), 115 (sftp), 25 (smtp), 22 (ssh).

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

CAA: From RFC 6844 (http:tools.ietf.org/html/rfc6844): "The Certification Authority Authorization (CAA) DNS Resource Record allows a DNS domain name holder to specify the Certification Authorities (CAs) authorized to issue certificates for that domain. Publication of CAA Resource 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 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 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 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 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 System Component: A individual element of a larger Certificate System used to process, approve issuance of, or store certificates or certificate status information. This includes the database, database server, storage devices, certificate hosting services, registration authority systems, and any other element used in certficiate management.

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.

Certificate Transparency (CT): Publicly operated record of certificate issuance.

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 State by at least two UN member nations.

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

CSPRNG: A random number generator intended for use in cryptographic system.

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.

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

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

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

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

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

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

Effective Date: 1 July 2012.

Embedded SCT: An SCT delivered via an X.509v3 extension within the certificate.

Enterprise RA: An employee or agent of an organization unaffiliated with the CA who authorizes issuance of Certificates to that organization.

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

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

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: An area (physical or logical) protected by physical and logical controls that appropriately protect the confidentiality, integrity, and availability of the CA's or Delegated Third Party Private Key or cryptographic hardware.

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.

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.

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.

Legal Entity: An association, corporation, partnership, proprietorship, trust, government entity or other entity with legal standing in a country's legal system.

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.

Offline: An air-gapped Certificate System or component that is only turned on to conduct certificate activity (i.e. issue / revoke a certificate, issue certificate revocation list, etc).

Online: Certificate Systems or components that are physcially and logically connected to the public and/or a private internet.

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

Parent Company: A company that Controls a Subsidiary Company.

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.

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 8.3.

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

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

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.

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.

Request Token: A value derived in a method specified by the CA which binds this demonstration of control to the certificate request.

- The Request Token SHALL incorporate the key used in the certificate request.
- A Request Token MAY include a timestamp to indicate when it was created.
- A Request Token MAY include other information to ensure its uniqueness.
- A Request Token that includes a timestamp SHALL remain valid for no more than 30 days from the time of creation.
- A Request Token that includes a timestamp SHALL be treated as invalid if its timestamp is in the future.
- A Request Token that does not include a timestamp is valid for a single use and the CA SHALL NOT re-use it for a subsequent validation.

The binding SHALL use a digital signature algorithm or a cryptographic hash algorithm at least as strong as that to be used in signing the certificate request.

Required Website Content: Either a Random Value or a Request Token, together with additional information that uniquely identifies the Subscriber, as specified by the CA.

Requirements: The Requirements found in this document.

Reserved IP Address: An IPv4 or IPv6 address that the IANA has marked as reserved:

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

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

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

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.

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

Signed Certificate Timestamp (SCT): A timestamp and promise from a Certificate Transparency operator to add the submitted certificate to the log within a specified time period.

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 Agreement or Terms of Use.

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.

Technically Constrained Subordinate CA Certificate: A Subordinate CA certificate which uses a combination of Extended Key Usage settings and Name Constraint settings to limit the scope within which the Subordinate CA Certificate may issue Subscriber or additional Subordinate CA Certificates.

Terms of Use: Provisions regarding the safekeeping and acceptable uses of a Certificate issued in accordance with these Requirements when the Applicant/Subscriber is an Affiliate of the CA or is the CA.

Test Certificate: A Certificate with a maximum validity period of 30 days and which: (i) includes a critical extension with the specified Test Certificate CABF OID, or (ii) is issued under a CA where there are no certificate paths/chains to a root certificate subject to these Requirements.

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.

353 **Valid Certificate**: A Certificate that passes the validation procedure specified in RFC 5280.

354 **Validation Specialists**: Someone who performs the information verification duties specified by these
355 Requirements.

356 **Validity Period**: The period of time measured from the date when the Certificate is issued until the
357 Expiry Date.

358 **Wildcard Certificate**: A Certificate containing an asterisk (*) in the left-most position of any of the
359 Subject Fully-Qualified Domain Names contained in the Certificate.

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

362 1.6.2 Acronyms

Acronym	Meaning
AICPA	American Institute of Certified Public Accountants
CA	Certification Authority
CAA	Certification Authority Authorization
ccTLD	Country Code Top-Level Domain
CICA	Canadian Institute of Chartered Accountants
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DBA	Doing Business As
DNS	Domain Name System
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
IM	Instant Messaging
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
ISO	International Organization for Standardization
NIST	(US Government) National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
RA	Registration Authority
S/MIME	Secure MIME (purpose Internet Mail Extensions)
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security

Acronym	Meaning
VOIP	Voice Over Internet Protocol

1.6.3 References

ETSI EN 319 403, Electronic Signatures and Infrastructures (ESI); Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers

ETSI EN 319 411-1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements

ETSI TS 102 042, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.

FIPS 140-2, Federal Information Processing Standards Publication - Security Requirements For Cryptographic Modules, Information Technology Laboratory, National Institute of Standards and Technology, May 25, 2001.

ISO 21188:2006, Public key infrastructure for financial services – Practices and policy framework.

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.

RFC6960, Request for Comments: 6960, X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP. Santesson, Myers, Ankney, Malpani, Galperin, Adams, June 2013.

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.509, Recommendation ITU-T X.509 (10/2012) | ISO/IEC 9594-8:2014 (E), Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks.

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 Federal PKI Policy Authority will review and update this Certificate Policy at least every 365 days to ensure compliance with CA/Browser Forum Baseline requirements. After review and approval, the CP document version number and a dated changelog entry shall be added even if no changes were deemed necessary.

The review and update shall include any changes needed to address:

- US Federal Government mission needs and changes to procedures to support the missions
- CA/Browser Forum Baseline Requirements updates

If changes to CA/Browser Forum Baseline requirements are made and have applicable requirements which require compliance earlier than 365 days from the last update, the Federal PKI Policy Authority will update the policy to meet those compliance timeframes and ensure all CA's and associated CA Certification Practice Statements are updated.

Each CA SHALL develop, implement, enforce, and update at least every 365 days a Certification Practice Statement (CPS) that describes in detail how the CA implements the requirements of this CP.

An annual self-assessment shall be conducted by any CA operating under this Certificate Policy and the accompanying CA CPS to show compliance with the latest version of this certificate policy and the CA/Browser Forum Baseline Requirements. The CA shall indicate the self-assessment by incrementing the CPS version number and adding a dated changelog entry to the change record.

2.1 Repositories

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

The CA shall post all CA certificates and CRLs issued by the CA in a repository that is publicly accessible through all Uniform Resource Identifier (URI) references asserted in valid certificates issued by that CA. The CA SHALL document the Uniform Resource Identifiers for CA certificates and CRLs in the CPS.

2.2 Publication of information

The Federal PKI Policy Authority SHALL publicly post this Certificate Policy on <INSERT URL>, ensuring it is readily accessible on a 24x7 basis.

All CAs SHALL publicly disclose redacted Certification Practice Statement through a readily accessible online means that is available on a 24x7 basis. The CA SHALL publicly disclose its CA practices and audits to the extent required by the CA's audit scheme (see Section 8.1). The disclosures SHALL include all the material required by RFC 3647, and SHALL be structured in accordance with or RFC 3647. The Certification Practice Statement SHALL state the CA's 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 Federal PKI Policy Authority and/or a designee and/or the CAs SHALL publish test Web pages that allow Application Software Suppliers to test their software with Subscriber Certificates from the Issuing CAs that chain up to the publicly trusted Root Certificate. At a minimum, separate Web pages SHALL be published showing Subscriber Certificates that are (i) valid, (ii) revoked, and (iii) expired.

2.3 Time or frequency of publication

The Federal PKI Policy Authority and CAs shall update and publish the Certificate Policy and Certification Practices Statements in accordance with Section 2.0.

All CAs approved to issue a CA certificate SHALL post to the Repository any issued CA certificate as soon as possible after issuance but no later than 15 days after issuance. The Federal PKI Policy Authority or designee shall disclose the CA certificate and submit the CA certificate to trust stores and applicable databases, such as the Common CA Database, within thirty (30) days of issuance.

Each CA SHALL publish CRLs in accordance with Section 4.9.7.

2.4 Access controls on repositories

Each CA shall make its Repository publicly available in a read-only manner.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

This policy restricts the subject names of CAs. CAs that issue certificates under this policy SHALL have distinguished names using geo-political names consisting of country, organization, and common name. Organization units may only be used with approval by the Policy Authority.

Subscriber certificates issued under this policy SHALL use distinguished names and subject alternative names that comply with Section 7.1.4, and the certificate profiles.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers are not identified in Domain Validation certificates. Only the country (US) and domain name is included in the subject information.

Subscribers are partially identified in Organizational Validation certificates. The organization and location of the U.S. Government are included in the subject information. All Organizational Validation certificates only include an organization of U.S. Government and no additional organizational unit information.

Relying parties should consider certificates to be issued by the U.S. Government for U.S. Government assets and all Subscribers to be affiliated with the U.S. Government.

3.1.4 Rules for interpreting various name forms

Distinguished names in certificates are interpreted using the X.500 Standard and the ASN.1 syntax.

The subject name in CA certificates SHALL match the issuer name in certificates issued by the subject, as required by RFC 5280.

3.1.5 Uniqueness of names

The common name attribute for Root CA(s) SHALL be unique. The common name attribute for Subordinate CAs SHALL be unique from all other Subordinate CAs.

3.1.6 Recognition, authentication, and role of trademarks

CAs operating under this policy shall not issue a certificate that knowingly infringes any trademark.

The Policy Authority shall resolve disputes involving names and trademarks.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

Issuing CA's SHALL describe the method(s) used to prove possession of private keys in the Certification Practice Statement(s).

Example: The CA verifies the digital signature on a signed object. The signed object is a PKCS#10 certification signing request.

3.2.2 Authentication of Organization and Domain Identity

All Domain Validation certificates issued under this Certificate Policy MAY include Subject Identity Information of countryName and SHALL NOT include any other Subject Identity Information with the exception of the required Common Name. If the Applicant requests a Domain Validation Certificate that will contain Subject Identity Information to include the 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.

All Organization Validation certificates issued under this Certificate Policy SHALL include Subject Identity Information of countryName **and** Organization **and** State and SHALL NOT include any other Subject Identity Information with the exception of the required Common Name. If the Applicant requests a Certificate that will contain Subject Identity Information comprised of the countryName field and Organization and State, 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 Section 3.2.2.1.

Issuing CA's SHALL describe these verification processes in the Certification Practice Statement(s).

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

3.2.2.1 Identity

Any Organization Validation certificates issued under this Certificate Policy are for U.S. Government mission purposes and for consumers, partners, and other relying parties to identify the U.S. as the subject. All Organization Validation certificates SHALL include Subject Identity Information of countryName **and** Organization **and** State and SHALL NOT include any other Subject Identity Information with the exception of the required Common Name. See Section 7.1.4.2.2.

If the Subject Identity Information is to include the name of our organization (o=U.S. Government), the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. Asserting U.S. Government as the organization SHALL be verified by the CA using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A third party database that is periodically updated and considered a Reliable Data Source such as the DotGov and DotMil Domain Name Registrars;
3. <not allowed>
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.

Practice Note: U.S. Government entities are in the jurisdiction of the U.S. Government. Verification of the domain to be part of the U.S. Government as the top level organization (o=U.S. Government) SHOULD suffice to assert the U.S. Government primary headquarter locations for address. This Certificate Policy relies upon the establishment of three branches of the U.S. Government as defined in the U.S. Constitution. All three branches of the U.S. Government have primary headquarters located in the city of Washington in the District of Columbia in the United States of America. *End Practice Note*

3.2.2.2 DBA/Tradename

Subject Identity Information SHALL NOT include a DBA or tradename.

3.2.2.3 Verification of Country

This Certificate Policy is restricted to the gTLDs for DotGov and DotMil, registered as the sub-category of *sponsored* TLDs (sTLDs) with ICANN.

DotGov is sponsored by the U.S. Government's General Services Administration. DotGov regulations are defined in 41 CFR Part 102-173. Under 41 CFR Part 102-173.30, registration in the DotGov domain is only available to official governmental organizations in the United States including Federal, State and local governments, and Native Sovereign Nations.

DotMil is sponsored by the U.S. Government's Department of Defense. The DotMil domain exists for the exclusive use of the Department of Defense and is referenced in Department of Defense Issuances Informational (DoDI) 8410.

The Domain Name Registrars for both DotGov and DotMil are managed by the U.S. Government.

This Certificate Policy asserts for all Certificate Authorities operating under this policy that the inclusion of subject:countryName in any Subscriber certificate is verified by:

- Section 3.2.2.3 of the CA/B Forum Baseline Requirements, option (c): information provided by the Domain Name Registrar
- Section 3.2.2.3 of the CA/B Forum Baseline Requirements, option (b): the ccTLD of the requested Domain Name. This CP asserts comparable controls for the sTLDs operated by the U.S. Government.

Issuing CA's SHALL describe these verification processes in the Certification Practice Statement(s).

3.2.2.4 Validation of Domain Authorization or Control

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

This Certificate Policy allows for procedures adhering to:

- 3.2.2.4.5 Domain Authorization Document
- 3.2.2.4.6 Agreed-Upon Change to Website
- 3.2.2.4.10 TLS Using a Random Number

Wildcard certificates are not allowed to be validated using 3.2.2.4.6 or 3.2.2.4.10. All wildcard certificates SHALL require a Domain Authorization Document signed by the Domain Contact authorizing the issuing of a wildcard certificate.

The CA SHALL confirm that, as of the date the Certificate issues, the CA has validated each Fully-Qualified Domain Name (FQDN) listed in the Certificate using at least one of the methods listed in Section 3.2.2.4.x.

Completed confirmations of Applicant authority may be valid for the issuance of multiple certificates over time. In all cases, the confirmation must have been initiated within the time period specified in the relevant requirement (Section 3.3.1 of this document) prior to certificate issuance. For purposes of domain validation, the term Applicant includes the Applicant's U.S. Government Department, Agency, Commission, component, or other organizational unit defined in United States Code.

Note: FQDNs may be listed in Subscriber Certificates using dNSNames in the subjectAltName extension or in Subordinate CA Certificates via dNSNames in permittedSubtrees within the Name Constraints extension.

3.2.2.4.1 [Reserved]

Not allowed as of the Effective Date of this Certificate Policy.

3.2.2.4.2 [Reserved]

Not allowed as of the Effective Date of this Certificate Policy.

3.2.2.4.3 [Reserved]

Not allowed as of the Effective Date of this Certificate Policy.

3.2.2.4.4 [Reserved]

Not allowed as of the Effective Date of this Certificate Policy.

3.2.2.4.5 Domain Authorization Document

Confirming the Applicant's control over the requested FQDN by relying upon the attestation to the authority of the Applicant to request a Certificate contained in a Domain Authorization Document. The Domain Authorization Document SHALL substantiate that the communication came from the Domain Contact. The CA SHALL verify that the Domain Authorization Document was either (i) dated on or after

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

3.2.2.4.6 Agreed-Upon Change to Website

Confirming the Applicant's control over the requested 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 or on a web page in the form of a meta tag. The entire Required Website Content MUST NOT appear in the request used to retrieve the file or web page, or
2. The presence of the Request Token or Request Value contained in the content of a file or on a webpage in the form of a meta tag 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 30 days.

Note: Examples of Request Tokens include, but are not limited to: (i) a hash of the public key; (ii) a hash of the Subject Public Key Info [X.509]; and (iii) a hash of a PKCS#10 CSR. A Request Token may also be concatenated with a timestamp or other data.

The CA SHALL define in its CPS the format of Request Tokens it accepts and SHALL document the "/.well-known/pki-validation/" directory and any other paths registered with IANA.

3.2.2.4.7 [Reserved]

3.2.2.4.8 [Reserved]

3.2.2.4.9 [Reserved]

3.2.2.4.10. TLS Using a Random Number

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

3.2.2.5 Authentication for an IP Address

Not allowed as of the Effective Date of this Certificate Policy. IP Addresses are not allowed in the certificate profiles under this Certificate Policy.

3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName, the CA SHALL establish and follow a documented procedure and technical controls that determines if the wildcard character occurs in the first label position to the left of the DotGov and DotMil suffixes (e.g. *.gov, *.mil). If a wildcard would fall within the label immediately to the left of the DotGov and DotMil suffixes

(e.g. *.gov, *.mil), CAs SHALL refuse issuance. All CAs are prohibited from issuing any Wildcard Certificate to the entire gTLDs for DotGov and / or DotMil.

Wildcard certificates are not allowed to be validated using 3.2.2.4.6 or 3.2.2.4.10. All wildcard certificates SHALL require a Domain Authorization Document (3.2.2.4.5) by the Domain Contact authorizing the issuing of a certificate that includes a wildcard domain.

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 or affiliated government agencies do not qualify as a Reliable Data Source if the primary purpose of the database is to collect information for the purpose of fulfilling the validation requirements under this Section 3.2.

3.2.2.8 CAA Records

When processing CAA records, CAs SHALL process the issue, issuewild, and iodef property tags as specified in RFC 6844, although they are not required to act on the contents of the iodef property tag. Additional property tags MAY be supported, but SHALL NOT conflict with or supersede the mandatory property tags set out in this document. CAs SHALL respect the critical flag and not issue a certificate if they encounter an unrecognized property with this flag set.

RFC 6844 requires that CAs "MUST NOT issue a certificate unless either (1) the certificate request is consistent with the applicable CAA Resource Record set or (2) an exception specified in the relevant Certification Practices Statement applies."

For issuances conforming to this Certificate Policy, CAs SHALL NOT rely on any exceptions specified in their respective CPS unless they are one of the following:

- CAA checking is optional for certificates for which a Certificate Transparency pre-certificate was created and logged in at least two public logs, and for which CAA was checked.
- CAA checking is optional if the CA or an Affiliate of the CA is the DNS Operator (as defined in RFC 7719) of the domain's DNS.

CAs are permitted to treat a record lookup failure as permission to issue if:

- the failure is outside the CA's infrastructure;
- the lookup has been retried at least once; and
- the domain's zone does not have a DNSSEC validation chain to the ICANN root.

CAs SHALL document potential issuances that were prevented by a CAA record in sufficient detail to provide feedback on the circumstances, and SHOULD dispatch reports of such issuance requests to the contact(s) stipulated in the CAA iodef record(s), if present. CAs are not expected to support URL schemes in the iodef record other than mailto: or https:.

3.2.3 Authentication of individual identity

Subscriber certificates identifying and authenticating natural born persons or individual identity SHALL NOT be issued under this policy.

3.2.4 Non-verified subscriber information

Non-verified subscriber information SHALL NOT be asserted in any certificates under this Certificate Policy.

3.2.5 Validation of authority

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, human resource offices, information technology offices, or other division 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 or Certification

CAs SHALL NOT have Cross Certificate(s) that identify the CA as the Subject without explicit written permission of the Policy Authority. Any Cross Certificates SHALL be disclosed publicly, submitted to one or more Certificate Transparency Logs, published to the Repository, and identified in the update to the CPS.

3.3 Identification and authentication for re-key requests

Re-key requests are not allowed under this policy. All requests are treated as new certificate requests.

3.3.1 Identification and authentication for routine re-key

See Section 3.3

3.3.2 Identification and authentication for re-key after revocation

See Section 3.3

3.4 Identification and authentication for revocation request

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

In accordance with Section 5.5.2, all CAs 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. All CA SHALL use this information to identify subsequent suspicious certificate requests.

For the Root and Subordinate CAs:

- An application for a CA certificate shall be submitted by an authorized representative of the applicant CA.

For end entity certificates:

- A certificate application shall be submitted to the CA by the Subscriber, an Applicant Representative, or an RA on behalf of the Subscriber.

4.1.2 Enrollment process and responsibilities

For the Root and Subordinate CAs:

- The Policy Authority is responsible for approving or denying requests for CA certificate issuances.

For all CAs, prior to the issuance of any 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 certificate request SHALL 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.

The CA SHALL be responsible for validating the information in the certificate request and the identity evidence to ensure the information is:

- properly formed
- accurate

- meets the requirements for the type of certificate requested: a device Domain Validation SSL end entity certificate, a device Organizational Validation SSL end entity certificate, a CA Certificate, or a Certificate Status Server (OCSP) signing certificate

All communications supporting the certificate application and issuance process SHALL be authenticated and protected from modification; any electronic transmission of shared secrets shall be protected. Communications may be electronic or out-of-band. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair SHALL be used. Out-of-band communications SHALL protect the confidentiality and integrity of the data.

All CAs SHALL shall specify the procedures for validating information and identity evidence in the CA CPS.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

All CAs SHALL establish and follow a documented procedure for verifying all data requested for inclusion in the Certificate by the Applicant.

For end entity Domain Validation SSL certificates and end entity Organizational Validation SSL certificates:

- The Applicant information SHALL include at least one Fully-Qualified Domain Name to be included in the Certificate's SubjectAltName extension
- All Fully-Qualified Domain Names to be included in the Certificate's SubjectAltName extension SHALL be verified in accordance with Section 3.2 before issuance of the certificate
- CAA records for DotGov and DotMil domains SHALL be checked prior to issuance of any certificate and the CA SHALL act in accordance to the rules in the CAA records if present. The CA SHALL identify in Section 4.2 of the CPS the Issuer Domain Name(s) used for CAA records.

The CA MAY use the documents and data provided in Section 3.2 to verify certificate information, provided that the CA obtained the data or document from a source specified under Section 3.2 no more than 825 days prior to issuing the Certificate.

All Subordinate CAs SHALL develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests for .GOV (DotGov) and .MIL (DotMil) assets prior to the Certificate's approval.

Delegated Third Parties are not allowed under this policy.

4.2.2 Approval or rejection of certificate applications

This Certificate Policy is restricted to be applicable to, and technically constrained, for DotMil and DotGov assets.

CAs SHALL reject all certificate applications containing any FQDNs that are not under the gTLDs for DotGov and DotMil.

Approval of certificate applications requires successful completion of validation per Section 3.2.

In accordance with Section 5.5.2, all CAs 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. All CAs SHALL use this information to identify subsequent suspicious certificate requests and MAY use it as the basis for rejecting a certificate request.

4.2.3 Time to process certificate applications

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

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. Issuance of a CA certificate by the Root CA SHALL require written authorization by the Policy Authority.

All end entity certificates for Domain Validation SSL and Organizational Validation SSL SHALL assert a Certificate Transparency (CT) Signed Certificate Timestamp (SCT) via the x509v3 certificate extension.

The Issuing CA SHALL submit a precertificate to a minimum of TWO Certificate Transparency Logs for certificates with a validity period less than or equal to 395 days. The Issuing CA SHALL submit a precertificate to a minimum of THREE Certificate Transparency Logs for certificates with a validity period greater than 395 days and less than or equal to 825 days. There is no limit on the maximum number of CT Logs which may be submitted to.

- At least one of the Certificate Transparency Logs SHALL be a CT Log operated by Google.
- At least one of the Certificate Transparenty Logs SHALL be a CT Log NOT operated by Google.

The Issuing CA SHALL include at least the same number and variety of SCTs in the x509v3 certificate extension for the end entity certificate issued.

Information included in the end entity certificates SHALL NOT be redacted prior to submission to the Certificate Transparency Logs.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The CA SHALL issue the certificate according to the certificate requesting protocol used by the device (this may be automated) and, if the protocol does not provide inherent notification, also notify the authorized representative of the issuance.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

Failure of the subscriber to object to the certificate or its contents shall constitute acceptance of the certificate.

4.4.2 Publication of the certificate by the CA

As specified in Section 2.1, all CA certificates SHALL be published in repositories. All CA certificates SHALL be published to the repositories within 24 hours of issuance. CAs SHALL log all end entity certificates in a minimum of two (2) Certificate Transparency Log servers as outlined in Section 4.3.1.

4.4.3 Notification of certificate issuance by the CA to other entities

See Section 4.4.2.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

The intended scope of usage for a private key shall be in accordance with the certificate profiles included with this Certificate Policy.

4.5.2 Relying party public key and certificate usage

All CAs operating under this policy provide revocation information in accordance with Section 4.9.7 and Section 4.9.9.

It is recommended that relying parties process and comply with this information whenever using certificates in a transaction.

4.6 Certificate renewal

Renewal is defined as the re-issuance of a certificate with no changes to the public key, no changes to the identity information, and a new validity period for the certificate.

4.6.1 Circumstance for certificate renewal

CA certificates SHALL NOT be renewed. End entity Domain Validation SSL certificates and end entity Organizational Validation SSL certificates SHALL NOT be renewed. Certificate renewal requests SHALL be treated as new applications and information verified in accordance with Section 4.2.1

Online Certificate Status Protocol (OCSP) Delegated responder certificates MAY be renewed.

4.6.2 Who may request renewal

The Policy Authority SHALL request that CAs routinely process OCSP Delegated Responder certificate renewal requests at the time the original certificate is requested by the Administrator.

4.6.3 Processing certificate renewal requests

The CA SHALL verify that the OCSP Delegated Responder certificate expiration date SHALL NOT exceed 825 days from the date of initial certificate issuance.

4.6.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.6.5 Conduct constituting acceptance of a renewal certificate

See Section 4.4.1.

4.6.6 Publication of the renewal certificate by the CA

See Section 4.4.2.

4.6.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.2.

4.7 Certificate re-key

Re-key is defined as the issuance of a certificate with a new public key, no changes to the identity information, and a new validity period for the certificate.

4.7.1 Circumstance for certificate re-key

All Certificates under this policy SHALL NOT be re-keyed. Certificate re-key requests SHALL be treated as new applications and information verified in accordance with Section 4.2.1

4.7.2 Who may request certification of a new public key

Not applicable.

4.7.3 Processing certificate re-keying requests

Not applicable.

4.7.4 Notification of new certificate issuance to subscriber

Not applicable.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

Not applicable.

4.7.6 Publication of the re-keyed certificate by the CA

Not applicable.

4.7.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate modification

Modification is defined as the re-issuance of a certificate with the same public key, and changes to the identity information or information in the certificate (i.e. policies, key usage) other than the validity period.

4.8.1 Circumstance for certificate modification

End entity Domain Validation SSL certificates and end entity Organizational Validation SSL certificates SHALL NOT be modified. Online Certificate Status Protocol (OCSP) Delegated responder certificates SHALL NOT be modified.

CA certificates MAY be modified to update attributes other than the public key. A CA certificate SHALL NOT be modified to add restrictions not in the original certificate unless all Subscriber certificates previously issued by the CA conform to the new restrictions.

4.8.2 Who may request certificate modification

See Section 4.1.1.

4.8.3 Processing certificate modification requests

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. Modification of a CA certificate by the Root CA SHALL require written authorization by the Policy Authority.

4.8.4 Notification of new certificate issuance to subscriber

See Section 4.3.2.

4.8.5 Conduct constituting acceptance of modified certificate

See Section 4.4.1.

4.8.6 Publication of the modified certificate by the CA

See Section 4.4.2.

4.8.7 Notification of certificate issuance by the CA to other entities

See Section 4.4.2.

4.9 Certificate revocation and suspension

4.9.1 Circumstances for revocation

4.9.1.1 Reasons for Revoking a Subscriber Certificate

The CA SHALL revoke a Certificate as rapidly as possible but 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 Sections 6.1.5 and 6.1.6;
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 in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked the right to use the Domain Name or the Domain Name Registrant has failed to renew the Domain Name under DotGov and/or DotMil gTLDs);
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 this Certificate Policy or the CA's 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 FPKI Policy Authority or 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).

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

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

1. The Subordinate CA requests revocation in writing;
2. The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
3. The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
4. The Issuing CA obtains evidence that the Certificate was misused;
5. The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this 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 FPKI Policy Authority or 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 Subscriber, RA, or Issuing CA can initiate revocation. Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the issuing CA of reasonable cause to revoke the certificate.

The Policy Authority SHALL direct any revocation of a CA certificate.

4.9.3 Procedure for revocation request

The CA SHALL provide a process for Subscribers to request revocation of their own Certificates. The process SHALL 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.

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.

A request to revoke a certificate shall identify the certificate to be revoked, explain the reason for revocation, and allow the request to be authenticated (e.g., digitally or manually signed).

4.9.4 Revocation request grace period

There is no revocation grace period.

4.9.5 Time within which CA must process the revocation request

The CA SHALL begin investigation of a of a Request for Revocation or a Certificate Problem Report immediately upon 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 Office of the Inspector General (OIG) official that a Web site violates Federal regulation should carry more weight than a complaint from a user alleging that they were unable to complete their transaction); and
4. Relevant legislation.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

(Note: Following certificate issuance, a certificate may be revoked for reasons stated in Section 4.9.1. Therefore, relying parties should check the revocation status of all certificates that contain a CDP or OCSP pointer.)

4.9.7 CRL issuance frequency

For the status of Subscriber Certificates:

- All CAs SHALL publish CRLs. On-line CAs SHALL update and reissue CRLs at least once every 24 hours and the value of the nextUpdate field MUST NOT be more than seven days beyond the value of the thisUpdate field

For the status of Subordinate CA Certificates:

- The CA SHALL update and reissue CRLs at least (i) once every 31 days and (ii) within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field SHALL NOT be more than 32 days beyond the value of the thisUpdate field.

4.9.8 Maximum latency for CRLs

CRLs shall be published within 4 hours of generation. Furthermore, each CRL shall be published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

4.9.9 On-line revocation/status checking availability

OCSP responses SHALL conform to RFC6960 and/or RFC5019. OCSP responses SHALL 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 RFC6960.

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.

For the status of Subscriber Certificates:

- The OCSP Responder SHALL update the information used to respond to requests within 4 hours of a new CRL being issued by the CA for all requests. OCSP responses from this service SHALL have a maximum expiration time of ten (10) days

For the status of Subordinate CA Certificates:

- The CA SHALL update information provided via an Online Certificate Status Protocol at least (i) every 31 days and (ii) within 24 hours after revoking a Subordinate CA Certificate.

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

4.9.11 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

See Section 4.9.1. When a CA certificate is revoked a CRL SHALL be issued within 24 hours of notification.

4.9.13 Circumstances for suspension

Certificates issued under this policy SHALL NOT be suspended.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

4.10.1 Operational characteristics

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

4.10.2 Service availability

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.

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

Private keys for certificates issued under this policy SHALL NOT be escrowed.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

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 SHALL 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 SHALL 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 SHALL include administrative, organizational, technical, and physical safeguards appropriate to the sensitivity of the Certificate Data and Certificate Management Processes. The security plan SHALL 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 SECURITY CONTROLS

CA equipment SHALL be protected from unauthorized access while the cryptographic module is installed and activated. The CA SHALL implement physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens SHALL be protected against theft, loss, and unauthorized use.

All the physical control requirements specified below apply equally to the Root CA and Subordinate CAs, and any remote workstations used to administer the CAs, except where specifically noted.

5.1.1 Site location and construction

The location and construction of the facility housing the CA equipment, as well as sites housing remote workstations used to administer the CAs, SHALL be consistent with facilities used to house high-value, sensitive information. The site location and construction, when combined with other physical security protection mechanisms such as guards, high security locks, and intrusion sensors, SHALL provide robust protection against unauthorized access to the CA equipment and records.

5.1.2 Physical access

At a minimum, the physical access controls for CA equipment and Certificate Status Authority (CSA) equipment, as well as remote workstations used to administer the CAs, SHALL:

- Ensure that no unauthorized access to the hardware is permitted.
- Ensure that all removable media and paper containing sensitive plain-text information is stored in secure containers.
- Be manually or electronically monitored for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer systems.

When not in use, removable cryptographic modules, activation information used to access or enable cryptographic modules, and CA equipment SHALL be placed in secure containers. Activation data SHALL be either memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module, and SHALL not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA.

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs SHALL occur if the facility is to be left unattended. At a minimum, the check SHALL verify the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when "open," and secured when "closed," and for the CA, that all equipment other than the repository is shut down).
- Any security containers are properly secured.
- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

A person or group of persons SHALL be made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance SHALL be maintained. If the facility is not continuously attended, the last person to depart SHALL initial a sign-

out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3 Power and air conditioning

The CA SHALL have backup capability sufficient to lock out input, finish any pending actions, and record the state of the equipment automatically before lack of power or air conditioning causes a shutdown.

The repositories (containing CA certificates and CRLs) SHALL be provided with uninterrupted power sufficient for a minimum of 6 hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water exposures

CA equipment SHALL be installed such that it is not in danger of exposure to water.

5.1.5 Fire prevention and protection

No Stipulation

5.1.6 Media storage

Media SHALL be stored so as to protect them from accidental damage (e.g., water, fire, or electromagnetic) and unauthorized physical access.

5.1.7 Waste disposal

Sensitive media and documentation that are no longer needed for operations SHALL be destroyed in a secure manner. For example, sensitive paper documentation SHALL be shredded, burned, or otherwise rendered unrecoverable.

5.1.8 Off-site backup

Full system backups sufficient to recover from system failure SHALL be made on a periodic schedule. Backups are to be performed and stored off-site not less than once per week. At least one full backup copy SHALL be stored at an off-site location (separate from CA equipment). Only the latest full backup need be retained. The backup SHALL be stored at a site with physical and procedural controls commensurate to that of the operational CA.

5.2 Procedural controls

5.2.1 Trusted roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously.

The requirements of this policy are defined in terms of four roles. Each CA shall maintain lists, including names, contact information, and copies of appointment memoranda of those who act in these trusted roles, and shall make them available during compliance audits. The CA will make this information a part of the permanent records of the CA. However, the CA shall not maintain personnel or investigative records requiring protection under the Privacy Act.

1. Administrator - authorized to install, configure, and maintain the CA; establish and maintain accounts; configure profiles and audit parameters; and generate component keys.
2. Officer - authorized to request or approve certificates or certificate revocations, and perform the Validation Specialist functions for quarterly reviews of issued certificates
3. Auditor – authorized to review, maintain, and archive audit logs.
4. Operator – authorized to perform system backup and recovery.

These four roles are employed at the CA. Separation of duties SHALL comply with 5.2.4, and requirements for two-person control with 5.2.2, regardless of the titles and numbers of Trusted Roles.

A detailed description of the responsibilities for each role:

The Administrator shall be responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts;
- Configuring certificate profiles or templates and audit parameters, and;
- Generating and backing up CA keys.

Administrators shall not issue certificates to subscribers.

The Officer (aka Registration Authority and / or Validation Specialist) shall be responsible for:

- Verifying the identity of subscribers and accuracy of information included in certificates pursuant to Section 3.2
- Performing the Validation Specialist functions for quarterly reviews of issued certificates
- Approving and executing the issuance of the certificates where inspection of the validation information is required, and
- Requesting, approving and executing the revocation of certificates

The Audit Administrator shall be responsible for:

- Reviewing, maintaining, and archiving audit logs;
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS;

The Operator shall be responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

5.2.2 Number of Individuals Required per Task

The CA 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.

Where multiparty control is required, at least one of the participants SHALL be an Administrator. All participants must serve in a trusted role as defined in section 5.2.1. Multiparty control SHALL NOT be achieved using personnel that serve in the Auditor trusted role.

5.2.3 Identification and authentication for each role

An individual SHALL identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity. All Trusted Roles SHALL use a unique credential created by or assigned to a single person for identification adn authentication.

5.2.4 Roles requiring separation of duties

Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA software and hardware SHALL identify and authenticate its users and enforce least privilege. The CA software and hardware SHALL ensure that no user can assume both the Administrator and Officer roles, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

All persons filling trusted roles SHALL be selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens. The requirements governing the qualifications, selection and oversight of individuals who operate, manage, oversee, and audit the CA SHALL be set forth in the CPS.

5.3.2 Background check procedures

Trusted role personnel SHALL, at a minimum, pass a background investigation covering the following areas: • Employment; • Education; • Place of residence; • Law Enforcement; and • References. The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Adjudication of the background investigation SHALL be performed by a competent adjudication authority using a process consistent with Executive Order 13467 or equivalent.

5.3.3 Training Requirements and Procedures

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.

5.3.4 Retraining frequency and requirements

All personnel in Trusted roles SHALL maintain skill levels consistent with the CA's training and performance programs.

All individuals responsible for PKI roles SHALL be made aware of changes in the CA operation. Any significant change to the operations SHALL have a training (awareness) plan, and the execution of such plan SHALL be documented. Examples of such changes are CA software or hardware upgrade, changes in automated security systems, and relocation of equipment.

Documentation SHALL be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job rotation frequency and sequence

No Stipulation

5.3.6 Sanctions for unauthorized actions

The CA SHALL take appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA that are not authorized in this CP, the CA CPS, or other published procedures.

5.3.7 Independent Contractor Controls

Delegated Third Party are not allowed under this policy.

Direct contractor personnel employed to operate any part of the CAs or perform functions pertaining to the infrastructure shall be subject to the same personnel requirements set forth in 5.3.2 of this CP.

5.3.8 Documentation supplied to personnel

Documentation sufficient to define duties and procedures for each role SHALL be provided to the personnel filling that role.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The CA 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.

1. 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.

1. 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 for Processing and Archiving Audit Logs

Review of the audit log SHALL be required at least once every 60 days.

Such reviews involve verifying that the log has not been tampered with and then briefly inspecting all log entries, with a more thorough investigation of any alerts or irregularities in the logs. A statistically significant portion of the security audit data generated by the CA since the last review SHALL be examined. This amount will be described in the CPS.

All significant events SHALL be explained in an audit log summary. Actions taken as a result of these reviews SHALL be documented.

5.4.3 Retention Period for Audit Logs

Audit logs SHALL be retained on-site until reviewed, in addition to being archived as described in section 5.5. The individual who removes audit logs from the CA system SHALL be an official different from the individuals who, in combination, command the CA signature key.

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 SHALL ensure audit logs are unalterable or maintain an integrity mechanism to identify any changes.

The security audit data SHALL not be open for reading or modification by any human, or by any automated process, other than those that perform security audit processing. CA system configuration and procedures must be implemented together to ensure that only authorized people archive or delete security audit data. Procedures must be implemented to protect archived data from deletion or destruction before the end of the security audit data retention period (note that deletion requires modification access). Security audit data SHALL be moved to a safe, secure storage location separate from the location where the data was generated.

5.4.5 Audit Log Backup Procedures

Audit logs and audit summaries SHALL be backed up at least monthly. A copy of the audit log SHALL be sent off-site on a monthly basis.

5.4.6 Audit Log Accumulation System (internal vs. external)

The audit log collection system may or may not be external to the CA system. Automated audit processes SHALL be invoked at system or application startup, and cease only at system or application shutdown. Audit collection systems SHALL be configured such that security audit data is protected against loss (e.g., overwriting or overflow of automated log files). Should it become apparent that an automated audit system has failed, and the integrity of the system or confidentiality of the information protected by the system is at risk, operations SHALL be suspended until the problem has been remedied.

5.4.7 Notification to event-causing subject

There is no requirement to notify a subject that an event was audited. Real-time alerts are neither required nor prohibited by this policy.

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.

5.5 Records archival

CAs operating under this policy must follow either the General Records Schedules established by the National Archives and Records Administration or an agency-specific schedule as applicable.

5.5.1 Types of records archived

The CA SHALL retain all documentation relating to certificate requests and the verification thereof, and all Certificates and revocation thereof, for a minimum of 10 years and 6 months after any Certificate based on that documentation ceases to be valid.

CA archive records SHALL be sufficiently detailed to determine the proper operation of the CA and the validity of any certificate - including those revoked or expired - issued by the CA. At a minimum, the following data SHALL be recorded for archive:

- CA accreditation (if applicable)
- Certificate policy
- Certification practice statement
- Contractual obligations and other agreements concerning operations of the CA
- System and equipment configuration
- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Revocation requests
- Subscriber identity authentication data
- Subscriber agreements
- Documentation of receipt of tokens
- All CRLs issued and/or published
- Other data or applications to verify archive contents
- Compliance Auditor reports
- Any changes to the Audit parameters, e.g. audit frequency, type of event audited
- Any attempt to delete or modify the Audit logs
- Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)
- All changes to the trusted public keys, including additions and deletions
- The export of private and secret keys (keys used for a single session or message are excluded)
- The approval or rejection of a certificate status change request
- Appointment of an individual to a Trusted Role
- Destruction of cryptographic modules
- All certificate compromise notifications
- Remedial action taken as a result of violations of physical security
- Violations of Certificate Policy
- Violations of Certification Practice Statement

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 a minimum of 10 years and 6 months without any loss of data after any Certificate based on that documentation ceases to be valid.

5.5.3 Protection of archive

No unauthorized user SHALL be permitted to write to, modify, or delete the archive. For the CA, archived records may be moved to another medium. The contents of the archive SHALL not be released

except in accordance with the Privacy Act of 1974 (as amended) and applicable Agency policies. Records of individual transactions may be released upon request of any subscribers involved in the transaction or their legally recognized agents. Archive media SHALL be stored in a safe, secure storage facility separate from the CA.

If the original media cannot retain the data for the required period, a mechanism to periodically transfer the archived data to new media SHALL be defined by the archive site.

Alternatively, a CA operating under this policy may retain data using whatever procedures have been approved by NARA for that category of documents. Applications required to process the archive data SHALL be maintained for a period that equals or exceeds the archive requirements for the data.

5.5.4 Archive backup procedures

No Stipulation

5.5.5 Requirements for time-stamping of records

CA archive records SHALL be automatically time-stamped as they are created. The system clocks used for time-stamping SHALL be maintained in synchrony with an authoritative time standard.

5.5.6 Archive collection system (internal or external)

Archive data may be collected in any expedient manner.

5.5.7 Procedures to obtain and verify archive information

Procedures, detailing how to create, verify, package, transmit, and store the CA archive information, SHALL be published in the CPS.

5.6 Key changeover

To minimize risk from compromise of a CA's private signing key, that key may be changed often. From that time on, only the new key will be used to sign CA and subscriber certificates. If the old private key is used to sign OCSP responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

After a CA performs a Key Changeover, the CA may continue to issue CRLs with the old key until all certificates signed with that key have expired.

When a CA updates its private signature key and thus generates a new public key, the CA SHALL notify the FPKI Policy Authority and subscribers of the change.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

CA organizations shall have an Incident Response Plan and a Disaster Recovery Plan.

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 (RTO);
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.

The FPKIPA shall be notified by the CAs operating under this policy of any security incident. A security incident or incident is defined as a violation or imminent threat of violation of the NPE CP, CPS, subscriber agreements, MOA, or any other document that governs the operations of the CA. A security incident may include but is not limited to the following:

- Suspected or detected compromise of Certificate Systems
- Suspected or detected compromise of a certificate status server (CSS) if:
  - The CSS certificate has a lifetime of more than 72 hours and
  - The CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension)
- Physical or electronic penetration of the Certificate Systems
- Successful denial of service attacks on the Certificate System components
- Any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL
- Suspected or detected issuance of fraudulent certificates used for unethical purposes such as but not limited to promoting malware or illegal software.
- Any certificate issuance not in compliance with NPE CP, CPS, or NPE Certificate Profiles.
- CA private key compromise.
- A known or reasonably known, publicly reported compromise of Certificate Systems
- Any other issue that the FPKIPA identifies as calling into question the CAs integrity or trustworthiness

In the event of a CA or certificate compromise or fraudulent mis-issuance, the CA shall notify the FPKIPA as soon as possible, but no later than 24 hours from the time the incident was discovered. An initial security incident report shall be submitted to the FPKI@GSA.gov email or communicated directly to the FPKIPA and include the following sections:

1. Which Certificate Systems or components were affected by the incident
2. The CA's interpretation of the incident.
3. Was the incident detected as part of normal operations. If not, explain why.
4. Who detected the incident or perpetrated if known
5. When the incident was discovered
6. Physical location of the incident, if applicable.
7. A partial or complete list of all certificates that were either mis-issued or not compliant with the CP/CPS as a result of the incident.

A final security incident report shall be submitted at a date specified by the FPKIPA to the same location as the initial incident report and include all sections identified below.

1. A complete timeline of events.
2. If a compromise, a detailed description of the exploit and what and how infrastructure was compromised.
3. If the CA did not detect the incident, why not.
4. What specific remedial measures were taken or will take to address the underlying cause including specific CP/CPS updates.
5. Other information appropriate to understand the incident such as system or vendor documentation or other material.
6. Proof the mis-issued certificates were revoked.
7. Who detected or perpetrated the incident.
8. If requested, log files.
9. Detailed description of how the incident was closed.

In coordination with the CA, the FPKIPA may conduct the following activities as part of an incident response.

- Communicate with affected parties or directly with affected organizations
- Publish notice of revocation
- Publicly publish a final security incident report on an approved government website.
- Require the CA to employ, at the CA expense, a third party investigator to investigate the security incident and prepare a final security incident report.
- Request specific reports at a periodic interval as determined by the FPKIPA
- Specify a due date for the CA to submit a final security incident report.

The FPKIPA shall notify the CA, in writing, of its intentions in response to the security incident seven (7) days prior to the action by the FPKIPA except under exceptional circumstances (as defined in the glossary) where the FPKIPA will make reasonable efforts to communicate with the CA prior to taking action. The CA may propose an alternate course of action and the FPKIPA may consider reasonable alternatives but reserves the right to reject any proposed course of action not in the government's best interest.

Note: The FPKIPA will follow individual Application Trusted Root Program requirements to report security concerns.

5.7.2 Recovery Procedures if Computing resources, software, and/or data are corrupted

When computing resources, software, and/or data are corrupted, CAs operating under this policy SHALL respond as follows:

- Before returning to operation, ensure that the system's integrity has been restored.
- If the CA signature keys are not destroyed, CA operation SHALL be reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule.
- If the CA signature keys are destroyed, CA operation SHALL be reestablished as quickly as possible, giving priority to the generation of a new CA key pair.

5.7.3 Recovery Procedures after Key Compromise

In the event of a CA private key compromise, the following operations MUST be performed.

- The FPKI Policy Authority SHALL be immediately informed, as well as any superior CAs and any entities known to be distributing the CA certificate.
- The CA MUST generate new keys.
- The superior CA must be revoke the subordinate CA certificate within seven (7) days.
- All subscriber certificates MUST be revoked within twenty-four (24) hours.

If the CA distributed the private key in a Trusted Certificate, the CA SHALL perform the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate
- Initiate procedures to notify subscribers of the compromise.

Subscriber certificates may be renewed automatically by the CA under the new key pair, or the CA may require subscribers to repeat the initial certificate application process.

5.7.4 Business continuity capabilities after a disaster

For the Root CA, recovery procedures SHALL be in place to reconstitute the CA within six (6) hours of failure.

All other CAs operating under this policy SHALL have recovery procedures in place to reconstitute the CA within 72 hours of failure.

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the FPKI Policy Authority SHALL be notified at the earliest feasible time, and the FPKI Policy Authority SHALL take whatever action it deems appropriate.

Relying parties may decide of their own volition whether to continue to use certificates signed with the destroyed private key pending reestablishment of CA operation with new certificates.

5.8 CA or RA termination

1507 This section does not apply to CAs that have ceased issuing new certificates but are continuing to issue
1508 CRLs until all certificates have expired. Such CAs are required to continue to conform with all relevant
1509 aspects of this policy (e.g., audit logging and archives).

1510 When a CA operating under this policy terminates operations before all certificates have expired, the CA
1511 signing keys SHALL be surrendered to the FPKI Policy Authority.

1512 Any issued certificates that have not expired, SHALL be revoked and a final long term CRL with a
1513 nextUpdate time past the validity period of all issued certificates SHALL be generated. This final CRL
1514 SHALL be available for all relying parties until the validity period of all issued certificates has passed.
1515 Once the last CRL has been issued, the private signing key(s) of the CA to be terminated will be
1516 destroyed.

1517 Prior to CA termination, the CA SHALL provide archived data to an archive facility. As soon as possible,
1518 the CA will advise all other organizations to which it has issued certificates of its 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

In all cases, 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.

In all cases, the CA SHALL:

1. Generate the CA 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 that meet or exceed FIPS 140 Level 3 validation;
4. Log its CA key generation activities;
5. Maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in the Certificate Policy and Certification Practice Statement and its Key Generation Script.

The documentation of the procedure must be detailed enough to show that appropriate role separation was used and the CA key pair generation must create a verifiable audit trail that the security requirements for procedures were followed.

6.1.1.2 RA Key Pair Generation

RAs SHALL NOT generate key pairs.

6.1.1.3 Subscriber Key Pair Generation

The CA SHALL reject a certificate request if the requested Public Key does not meet the requirements set forth in Sections 6.1.5 and 6.1.6 or if it has a known weak Private Key (such as a Debian weak key, see http://wiki.debian.org/SSLkeys).

6.1.2 Private key delivery to subscriber

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

Subscribers SHALL generate their own keys in compliance with sections 6.1.5 and 6.1.6.

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

The public key and the subscriber's identity must be delivered securely to the CA for certificate issuance. The delivery mechanism shall bind the subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the certificate.

6.1.4 CA public key delivery to relying parties

When a Subordinate CA updates its signature key pair, the CA shall distribute the new public key in a secure fashion.

The Root CA certificate(s) shall be conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods for self-signed Root CA certificate delivery are:

- Loading a self-signed certificate onto tokens delivered to relying parties via secure mechanisms;
- Secure distribution of self-signed certificates through secure out-of-band mechanisms;
- Comparison of the hash of the self-signed certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism)

6.1.5 Key sizes

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

(1) Root CA Certificates

Digest algorithm	SHA-256, SHA-384 or SHA-512
Minimum RSA modulus size (bits)	4096
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

(2) Subordinate CA Certificates

Digest algorithm	SHA-256, SHA-384 or SHA-512

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

(3) Subscriber Certificates

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

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

6.1.6 Public key parameters generation and quality checking

RSA: The CA SHALL confirm that the value of the public exponent *e* shall be an odd positive integer such that:

- $2^{16} < e < 2^{256}$

The modulus SHALL also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: NIST SP 800-89 and NIST FIPS 186-4]

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 5.6.2.3.2 and 5.6.2.3.3, respectively, of NIST SP 800-56A: Revision 2]

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

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

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The CA SHALL implement physical and logical safeguards to prevent unauthorized certificate issuance. Protection of the CA 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 relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [FIPS 140-2]. Cryptographic modules shall be validated to a FIPS 140 level identified in this section.

- Cryptographic modules for CAs and OCSP responders SHALL be hardware modules validated as meeting FIPS 140-2 Level 3 or above

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

For all CAs:

- A single person shall not be permitted to activate or access any cryptographic module that contains the complete CA private signing key.
- CA signature keys may be backed up only under at least two-person control.
- Access to CA signing keys backed up for disaster recovery shall be under at least two-person control.
- The names of the parties used for two-person control shall be made available for inspection during Qualified Audits.

6.2.3 Private key escrow

For all CAs:

- The CA private keys SHALL never be escrowed

6.2.4 Private key backup

For all CAs:

- The CA private signature keys SHALL be backed up under the same multiperson control as the original signature key.
- At least one copy of the private signature key shall be stored off-site.
- All copies of the CA private signature key shall be accounted for and protected in the same manner as the original.
- Backup procedures shall be included in the CA's CPS

See Section 5.2.2.

6.2.5 Private key archival

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

All CAs shall generate their own keys in FIPS 140 validated cryptographic modules, in compliance with sections 6.1.5 and 6.1.6. CA private keys may be exported from the cryptographic module only to perform CA key backup procedures as described in section 6.2.4.1. At no time shall the CA private key exist in plaintext outside the cryptographic module. Private or symmetric keys used to encrypt other private keys for transport must be protected from disclosure.

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

All CAs SHALL protect their Private Keys in a system or device that has been validated as meeting at least FIPS 140 level 3 which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 Activating Private Keys

For the Root CA(s), signing key activation MUST implement multiparty control as specified in Section 5.2.2.

6.2.9 Deactivating Private Keys

Cryptographic modules that have been activated shall not be available to unauthorized access. After use, the cryptographic module shall be deactivated, e.g., via a manual logout procedure or automatically after a period of inactivity as defined in the CA's CPS. CA cryptographic modules SHALL be removed and stored in a secure container when not in use.

6.2.10 Destroying Private Keys

Individuals in trusted roles shall destroy all CA and OCSP private signature keys when the keys are no longer needed. All CAs operating under this policy shall document the private key destruction methods in their Certificate Practices Statement.

6.2.11 Cryptographic Module Capabilities

See Section 6.2.1

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

Root CA Certificates SHALL have a Validity Period no greater than 20 years. Subordinate CA Certificates SHALL have a Validity Period no greater than 10 years. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

All Subscriber Certificates SHALL have a Validity Period no greater than 825 days. Subscriber Certificates issued for delegated OCSP responders SHALL have a Validity Period no greater than 45 days.

6.4 Activation data

6.4.1 Activation data generation and installation

CA activation data may be user-selected by each of the multiple parties holding that activation data. If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation data protection

For all CAs, this CP makes no further stipulation beyond that specified in FIPS 140.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

Administrator privileges to all Certificate System components SHALL only be granted to the Administrator trusted role.

All CAs SHALL implement multifactor authentication for all Trusted Role accounts capable of directly causing certificate issuance or authenticating to Certificate Systems. All Trusted Roles SHALL use a unique credential created by or assigned to a single person for identification and authentication.

All CAs SHALL implement multifactor authentication for all access to component systems including operating system and software.

For all CAs and component systems including certificate status services operating under this policy, the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts SHALL include the following functionality:

- be configured to remove or disable all accounts, applications, services, protocols, and ports that are not used in the CA's operations;
- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles and implement least privilege controls;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes;
- support recovery from key or system failure; and

For remote workstations used to administer the CAs, the computer security functions listed below are required:

- authenticate the identity of users before permitting access to the system or applications;
- manage privileges of users to limit users to their assigned roles;
- generate and archive audit records for all transactions; (see section 5.4)
- enforce domain integrity boundaries for security critical processes; and
- support recovery from key or system failure; and
- configure workstations with inactivity time-outs to enforce account log out or lock the workstation when no longer in use;

All communications between any PKI trusted role and the CA shall be authenticated and protected from modification.

6.5.2 Computer security rating

No Stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

The system development controls for all CAs and any Registration Authority functions listed below are required:

- The CA hardware and software shall be dedicated to performing one task: the CA. There shall be no other applications, hardware devices, network connections, or component software installed that are not part of the CA operation. Where the CA operation supports multiple CAs, the hardware platform may support multiple CAs.
- Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the random selection of material at time of purchase or installation).
- Hardware and software shall be similarly limited and scanned for malicious code on first use and continuously thereafter.

6.6.2 Security management controls

The security management controls for all CAs and any Registration Authority functions listed below SHALL be implemented:

- The configuration of the CA system, in addition to any modifications and upgrades, SHALL be documented and controlled.
- Configurations SHALL be reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies.
- There SHALL be a mechanism for detecting unauthorized modification to the software or configuration. Configurations SHALL be reviewed on at least a weekly basis to determine whether any changes violated the CA's security policies.
- All system and trusted role accounts SHALL be reviewed at least every ninety (90) days. Any account that is no longer in use or necessary for operations SHALL be deactivated.
- A process SHALL be implemented that disables physical and logical access to a Certificate System by either a privileged user or a trusted role within 24 hours upon termination of the individual's employment or contracting relationship with the CA.
- All authentication credentials for any account or trusted role on a Certificate System SHALL be changed whenever authorization to access the account is changed or revoked.

6.6.3 Life cycle security controls

- Hardware and software shall be scanned for vulnerabilities at least every thirty (30) days
- Critical vulnerabilities shall be patched within thirty (30) days or less
- High vulnerabilities shall be patched within sixty (60) days or less
- CAs including Repositories and any Registration Authority system functions shall undergo penetration testing every ninety (90) days

6.7 Network security controls

Secure Zones are a physical or logical separation of Certificate Systems while a High Security Zone is a physical area where a private key or cryptographic equipment is stored. Each Zone is protected commensurate with its level of assurance. A High Security Zone may exist within a Secure Zone that is physically or logically separated from other Secure Zones.

For the Root CA, the CA SHALL be operated in a High Security Zone and in an offline (powered off, disconnected) or air-gapped (powered on, disconnected) state from all other networks.

For all CAs and any Registration Authority functions, the network security controls listed below are required:

- Secure Zones shall be implemented to secure Certificate Systems based on functional, logical, and physical (including location) relationships.
- The same security controls SHALL be applied to all systems co-located in the same Zone with a Certificate System.
- Security support systems SHALL be configured to protect systems and communications between systems inside Secure Zones and High Security Zones as well as with non-Certificate Systems to Delegated Third Parties, Public Networks, and other business partners.
- Only trusted roles SHALL have access to Secure and High Security Zones.
- A network guard, firewall, or filtering router shall protect network access to CA equipment.
- The network guard, firewall, or filtering router shall limit services allowed to and from the CA equipment to those required to perform CA functions.
- Protection of CA equipment shall be provided against known network attacks.

- All unused network ports and services shall be turned off. Any network software present on the CA equipment shall be necessary to the functioning of the CA application.
- Any boundary control devices used to protect the network on which equipment is hosted shall deny all but the necessary services to the equipment.
- Repositories, certificate status servers, and remote workstations used to administer the CAs shall employ appropriate network security controls.
- Networking equipment shall turn off unused network ports and services.
- Any network software present shall be necessary to the functioning of the equipment.
- The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA. Remote connections shall be restricted, except when:
    - the remote connection originates from a device owned by the CA and from a pre-approved IP address;
    - the connection is through a temporary, non-persistent and encrypted channel that is supported by multifactor authentication;
    - only allow connections through a designated intermediary device when the device is:
        - located within the CA's network;
        - secured according to this CP; and
        - mediates the remote connection.

6.8 Time-stamping

Asserted times shall be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events (see section 5.4.1).

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 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 (minimum of 8 octets) of output from a CSPRNG, not to exceed 20 octets.

7.1.1 Version number(s)

Certificates SHALL be of type X.509 v3.

7.1.2 Certificate Content and Extensions; Application of RFC 5280

This section specifies the additional requirements for Certificate content and extensions for Certificates generated after the Effective Date.

7.1.2.1 Root CA Certificate

a. basicConstraints (required)
Required/Optional: Required
This extension SHALL appear as a critical extension. The cA field SHALL be set true. The pathLenConstraint field SHALL NOT be present.

b. keyUsage (required)
Required/Optional: Required
This extension SHALL be present and MUST be marked critical. Bit positions for keyCertSign and cRLSign SHALL be set. If the Root CA Private Key is used for signing OCSP responses, then the digitalSignature bit MUST be set.

c. certificatePolicies
Required/Optional/Prohibited: Prohibited
This extension SHALL NOT be present.

d. extendedKeyUsage
Required/Optional/Prohibited: Prohibited
This extension SHALL NOT be present.

e. Subject Information / Subject Distinguished Name (required)
Required/Optional: Required See Section 7.1.4.3.1

7.1.2.2 Subordinate CA Certificate

a. certificatePolicies (required)
Required/Optional: Required
This extension SHALL be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (required)
Required/Optional: Required

b. cRLDistributionPoints (required)
Required/Optional: Required
This extension SHALL be present and SHALL NOT be marked critical. It SHALL contain the HTTP URL of the CA's CRL service. The HTTP URL included must be publicly accessible on the Internet.

c. authorityInformationAccess (required)
Required/Optional: Required
This extension SHALL be present. It SHALL NOT be marked critical, and it SHALL contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHALL also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2). At least one instance of the Id-ad-caIssuers accessMethod (accessMethod = 1.3.6.1.5.5.7.48.2) must be publicly accessible on the Internet and the artifacts served shall be in a BER or DER encoded "certs-only" CMS message as specified in [RFC2797]

d. basicConstraints (required)
Required/Optional: Required
This extension SHALL be present and SHALL be marked critical. The cA field SHALL be set true. The pathLenConstraint field SHALL NOT be present.

e. keyUsage (required)
Required/Optional: Required
This extension SHALL be present and SHALL 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.

f. nameConstraints (required)
Required/Optional: Required
This extension SHALL be present. This extension SHALL be marked critical. See section 7.1.5.

g. extkeyUsage (required)
Required/Optional: Required
This extension SHALL be present. This extension SHALL be marked non-critical.

All Subordinate CA Certificates are to be Technically constrained in accordance with section 7.1.5. The value id-kp-serverAuth [RFC5280] MUST be present, and the id-kp-clientAuth [RFC5280] MAY be present.

Other values MAY be present consistent with use for server authentication, with approval by the FPKI PA.

h. Subject Information / Subject Distinguished Name (required)
Required/Optional: Required
See Section 7.1.4.3.1

7.1.2.3 Subscriber Certificate

a. certificatePolicies (required)
Required/Optional: Required
This extension SHALL be present and SHOULD NOT be marked critical.

certificatePolicies:policyIdentifier (required)
Required/Optional: 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.

certificatePolicies:policyQualifiers:policyQualifierId (optional)

Required/Optional: Optional
The extension SHOULD be present and is Recommended.

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (optional)
Required/Optional: Optional
HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

b. cRLDistributionPoints (required)
Required/Optional: Required
This extension SHALL be present. It SHALL NOT be marked critical, and it SHALL contain the HTTP URL of the Issuing CA's CRL service.

c. authorityInformationAccess (required)
Required/Optional: Required
This extension SHALL be present. It SHALL NOT be marked critical, and it SHALL contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHALL also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

d. basicConstraints (required)
Required/Optional: Required
This extension SHALL be present. The cA field SHALL NOT be true.

e. keyUsage (required)
Required/Optional: Required
This extension SHALL be present and SHALL be marked critical.

Subscriber certificates used for server authentication SHALL include digitalSignature, and MAY include keyEncipherment and / or keyAgreement.

f. extKeyUsage (required)
Required/Optional: Required
This extension SHALL be present. It SHALL NOT be marked critical.

Either the value id-kp-serverAuth [RFC5280] or id-kp-clientAuth [RFC5280] or both values SHALL be present. id-kp-emailProtection [RFC5280] and anyEKU SHALL NOT be present.

Other values SHOULD NOT be present. Other values MAY be present consistent with use for server authentication, with approval by the FPKI PA.

7.1.2.4 All Certificates

All other fields and extensions SHALL 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 section 7.1.2.1, 7.1.2.2, or 7.1.2.3 unless the CA is aware of a reason for including the data in the Certificate and receives approval from the Policy Authority.

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 this Certificate Policy and the CA/Browser Forum Baseline Requirements.

7.1.3 Algorithm object identifiers

CAs SHALL NOT issue Subscriber Certificates utilizing the SHA-1 hash algorithm.

7.1.4 Name forms

7.1.4.1 Issuing CA Certificate Subject

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

CA Subject Distinguished Name SHALL conform to PrintableString string type in ASN.1 notation.

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 this Certificate Policy and the CA Certification Practice Statement to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

CAs SHALL NOT include IP Address in a Subject attribute. CAs SHALL NOT include a Domain Name in a Subject attribute except as specified in Section 3.2.2.4.

7.1.4.2.1 Subject Alternative Name Extension

Certificate Field: extensions:subjectAltName
Required/Optional/Prohibited: Required
Contents: This extension MUST contain at least one entry. Each entry MUST be a dNSName containing the Fully-Qualified Domain Name of a server. The CA MUST confirm that the Applicant controls the Fully-Qualified Domain Name or has been granted the right to use it by the Domain Name Registrant, as appropriate. This extension SHALL NOT include IP Address. This exentsion SHALL NOT include any Internal Name values.

Wildcard FQDNs are permitted.

7.1.4.2.2. Subject Distinguished Name Fields

a. **Certificate Field:** subject:commonName (OID 2.5.4.3)
Required/Optional/Prohibited: Required
Contents: This field SHALL contain a Fully-Qualified Domain Name that is one of the values contained in the Certificate's subjectAltName extension (see Section 7.1.4.2.1).

b. **Certificate Field:** subject:organizationName (OID 2.5.4.10)
Required/Optional/Prohibited: Optional
Contents: If present, the subject:organizationName field SHALL contain U.S. Government (o=U.S. Government).

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

d. **Certificate Field:** Number and street: subject:streetAddress (OID: 2.5.4.9)
Required/Optional/Prohibited: Prohibited

e. **Certificate Field:** subject:localityName (OID: 2.5.4.7)
Required/Optional/Prohibited: Prohibited

f. **Certificate Field:** subject:stateOrProvinceName (OID: 2.5.4.8)
Required/Optional/Prohibited:
Required if subject:organizationName is present.
Prohibited if the subject:organizationName is absent.
Contents: If present, the subject:stateOrProvinceName field MUST contain the Subject's state or province information as verified under Section 3.2.2.1. The subject:stateOrProvinceName field SHALL contain District of Columbia.

g. **Certificate Field:** subject:postalCode (OID: 2.5.4.17)
Required/Optional/Prohibited: Prohibited

h. **Certificate Field:** subject:countryName (OID: 2.5.4.6)
Required/Optional/Prohibited: Required if subject:organizationName is present.

Optional if subject:organizationName is absent.
Contents: If present, the subject:countryName SHALL contain the two-letter ISO 3166-1 country code of "US" associated with the location of the Subject verified under Section 3.2.2.1.

i. **Certificate Field:** subject:organizationalUnitName
Required/Optional/Prohibited: Prohibited

j. **Other Subject Attributes**
All other optional attributes, for the subject field, SHALL NOT be included. 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 Information - Root Certificates and Subordinate CA Certificates

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.

- Examples of Subject Distinguished Names for Root Certificates and Subordinate CA Certificates:
  - cn=U.S. Federal Device Root CA1, o=U.S. Government, c=US
  - cn=U.S. Federal Device Issuing CA1, o=U.S. Government, c=US

7.1.4.3.1 Subject Distinguished Name Fields

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

b. **Certificate Field:** subject:organizationName (OID 2.5.4.10)
Required/Optional: Required
Contents: This field SHALL be present and SHALL contain U.S. Government (o=U.S. Government).

c. **Certificate Field:** subject:countryName (OID: 2.5.4.6)
Required/Optional: Required
Contents: This field SHALL contain C=US

CA Certificate Subjects SHALL NOT include organizationalUnit unless approved by the Policy Authority.

All other optional attributes, for the CA Certificate Subject fields, SHALL NOT be included. 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.

7.1.5 Name constraints

All Subordinate CA Certificates SHALL be Technically Constrained.

For a Subordinate CA Certificate to be considered Technically Constrained, the certificate SHALL 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 SHALL NOT appear within this extension.

The Subordinate CA Certificate(s) SHALL include the id-kp-serverAuth extended key usage, and the Subordinate CA Certificate(s) SHALL include the Name Constraints X.509v3 extension with constraints on dNSName 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. The Subordinate CA Certificate MUST include at least one dNSName in permittedSubtrees. The permittedSubtrees for dNSName MUST be within the constraints of the top-level domains for:

- gov (DotGov)
- mil (DotMil)

The permittedSubtrees for dNSName MUST NOT contain any other dnsName ranges outside of the the DotGov or DotMil top-level domains.

b. For ipAddress, Subordinate CAs SHALL NOT issue subscriber certificates with an iPAddress. The Subordinate CA Certificate SHALL specify the entire IPv4 and IPv6 address ranges in excludedSubtrees. The Subordinate CA Certificate SHALL 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 SHALL also include within excludedSubtrees an iPAddress GeneralName of 32 zero octets (covering the IPv6 address range of ::0/0).

c. For DirectoryName, Subordinate CAs SHALL NOT issue subscriber certificates with DirectoryName.

A decoded example for issuance to the domain and sub domains of .mil (DotMil) by organization:- Example Department of Defense would be:-

X509v3 Name Constraints:
Permitted:
DNS:mil
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

A decoded example for issuance to the domain and sub domains of both .gov (DotGov) and .mil (DotMil) by organization:- Example Department of Defense would be:-

X509v3 Name Constraints:
Permitted:
DNS:mil
DNS:gov
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

7.1.6 Certificate policy object identifier

7.1.6.1. Reserved Certificate Policy Identifiers

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates, as they relate to the identification of Certificate Policy.

The following Certificate Policy identifiers are registered under the CA/Browser Forum and reserved for use. These Certificate Policy Identifiers are a **required** means of asserting compliance with the CA/Browser Forum Baseline Requirements as follows:

- Domain Validated:
  - {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 or Section 3.2.3.

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

- Organization Validated:
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) organization-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 SHALL also include organizationName, stateorProvinceName and countryName in the Subject field in accordance with Section 7.1.4.2.2. All information shall be verified in accordance with Section 3.2.2.1.

Certificates under this policy SHALL NOT assert the Individual Validated Certificate Policy identifiers reserved by the CA/Browser Forum.

- {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) baseline-requirements(2) individual-validated(3)} (2.23.140.1.2.3)

7.1.6.2. Root CA Certificates

A Root CA Certificate SHALL NOT contain the certificatePolicies extension.

7.1.6.3 Subordinate CA Certificates

All Subordinate CA's SHALL be an Affiliate as defined in this CP.

A Certificate issued to a Subordinate CA:

1. SHALL include the CA/B Forum reserved identifiers to indicate the Subordinate CA's compliance with the CA/Browser Forum Baseline Requirements, and

2. SHALL include an identifier defined in Section 1.2 to indicate the Subordinate CA's compliance with this Policy

A Subordinate CA SHALL represent, in its Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with the CA/Browser Forum Baseline Requirements are issued and managed in accordance with the CA/Browser Forum Baseline Requirements. A Subordinate CA SHALL represent, in its Certification Practice Statement, that all Certificates containing a policy identifier indicating compliance with this Certificate Policy are issued and managed in accordance with this Certificate Policy.

7.1.6.4 Subscriber Certificates

A Certificate issued to a Subscriber SHALL contain one policy identifier, defined by this CP in Section 1.2, in the Certificate's certificatePolicies extension that indicates adherence to and compliance with this Certificate Policy. CAs SHALL also assert one of the CA/B Forum Reserved Policy OIDs in such Certificates.

Subscriber certificates SHALL contain certificate policy identifier(s) for either domain validated policies or organization validated policies but SHALL NOT assert certificate policy identifiers for both.

The issuing CA SHALL document in its Certification Practice Statement that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with the CA/Browser Forum Baseline Requirements and this Certificate Policy.

7.1.7 Usage of Policy Constraints extension

Subordinate CAs MAY assert policy constraints in the CA certificates.

7.1.8 Policy qualifiers syntax and semantics

Certificates issued under this CP MAY contain policy qualifiers.

7.1.9 Processing semantics for the critical Certificate Policies extension

Certificates issued under this policy SHALL NOT contain a critical certificate policies extension.

7.2 CRL profile

7.2.1 Version number(s)

The CAs SHALL issue X.509 Version two (2) CRLs.

7.2.2 CRL and CRL entry extensions

a. reasonCode (required)
Required/Optional: Required
This entry extension SHALL be present. The reasonCode value SHALL be populated in accordance with

Section 4.9.1 for revocation reasons encompassing Key Compromise (reasonCode: keyCompromise) or CA Compromise (reasonCode: cACompromise).

7.3 OCSP profile

7.3.1 Version number(s)

OCSP Responders operated under this policy shall use OCSP version 1.

7.3.2 OCSP extensions

This section specifies the additional requirements for Certificate contents for Online Certificate Status Protocol certificates, and extensions for OCSP status server extension and responses.

a. certificatePolicies (required)
Required/Optional: Required

This extension SHALL be present and SHALL NOT be marked critical.

certificatePolicies:policyIdentifier (required)
Required/Optional: Required
The certificate SHALL include at least one certificate policy OID defined or listed in Section 1.2 of this CP and SHALL include all the certificate policy OIDs for all certificates issued by the Issuing CA and covered by the OCSP responses

certificatePolicies:policyQualifiers:policyQualifierId (optional)
Required/Optional: Optional
The extension SHOULD be present and is Recommended.

- id-qt 1 [RFC 5280].

certificatePolicies:policyQualifiers:qualifier:cPSuri (optional)
Required/Optional: Optional
HTTP URL for the Subordinate CA's Certification Practice Statement, Relying Party Agreement or other pointer to online information provided by the CA.

b. authorityInformationAccess (required)
Required/Optional: Required
This extension SHALL be present. It SHALL NOT be marked critical, and it SHALL contain the HTTP URL of the Issuing CA's OCSP responder (accessMethod = 1.3.6.1.5.5.7.48.1). It SHALL also contain the HTTP URL of the Issuing CA's certificate (accessMethod = 1.3.6.1.5.5.7.48.2).

c. basicConstraints
Required/Optional/Prohibited: Prohibited
This extension SHALL NOT be present.

d. keyUsage (required)
Required/Optional: Required
This extension SHALL be present. It SHALL be marked critical.

Certificates used for signing certificate status services (online certificate status protocol) SHALL include the value digitalSignature.

Other values SHALL NOT be present.

e. extKeyUsage (required)
Required/Optional: Required
This extension SHALL be present. It SHALL be marked critical.

It SHALL contain the value id-kp-OCSPSigning {1 3 6 1 5 5 7 3 9}.

Other values SHALL NOT be present.

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

The Certificate Authorities (X.509v3 basicConstraints extension, with the cA boolean set to true) operated under this Certificate Policy are Technically Constrained in line with section 7.1.5. They are audited in line with section 8.7.

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.

Before issuing Publicly-Trusted Certificates, any 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

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 the WebTrust standard) licensed by WebTrust;
5. Bound by law, government regulation, or professional code of ethics; and
6. 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

The compliance auditor either shall be a private firm that is independent from the entities (CA and RAs) being audited, or it shall be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Federal agency Inspector General. To insure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining the entity's CA Facility or certificate practices statement. The FPKI Policy Authority shall determine whether a compliance auditor meets this requirement.

The operating Agency and Management Authority of each CA is responsible for identifying and engaging a qualified auditor.

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 / ETSI EN 319 411-1; or

Whichever scheme is chosen, it SHALL 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 SHALL be conducted by a Qualified Auditor, as specified in Section 8.3.

There is no Delegated Third Party allowed under this Certificate Policy.

8.5 Actions taken as a result of deficiency

When the compliance auditor finds a discrepancy between the requirements of this CP or the stipulations in the CPS and the design, operation, or maintenance of the CAs, the following actions shall be performed: • The compliance auditor shall note the discrepancy; • The compliance auditor shall notify the responsible party promptly; and • The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKI Policy Authority.

Depending upon the nature and severity of the discrepancy, and how quickly it can be corrected, the FPKI Policy Authority may decide to temporarily halt operation of the CA or RA, to revoke a certificate issued to the CA or RA, or take other actions it deems appropriate. A compliance audit may be required to confirm the implementation and effectiveness of the remedy.

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. 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.

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.

During the period in which a Technically Constrained Subordinate CA issues Certificates, the CA which signed the Subordinate CA SHALL monitor adherence to the this 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.

There is no Delegated Third Party allowed under this Certificate Policy.

9. OTHER BUSINESS AND LEGAL MATTERS

This section contains the CA / Browser Forum Baseline Requirements and has not been modified. Additions to Business and Legal Matters to address Application Trusted Root Program requirements and U.S. Government provisions to meet public law requirements are under review and not included in this draft.

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

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 Agreement or Terms of Use for the Certificate;
2. All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root Certificate in software distributed by such Application Software Supplier; and
3. All Relying Parties who reasonably rely on a Valid Certificate. 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 the same entity or are Affiliated, the Applicant Representative acknowledged 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

9.6.2 RA representations and warranties

No stipulation.

9.6.3 Subscriber representations and warranties

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

The CA SHALL implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement MUST apply to the Certificate to be issued pursuant to the certificate request. 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 Agreement or Terms of Use.

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

1. **Accuracy of Information**: An obligation and warranty to provide accurate and complete information at all times to 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 assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device, e.g. password or token);
3. **Acceptance of Certificate**: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
4. **Use of Certificate**: An obligation and warranty to install the Certificate only on servers that are accessible at the subjectAltName(s) listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
5. **Reporting and Revocation**: An obligation and warranty to: (a) promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and (b) promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
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 Agreement or Terms of Use 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.

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

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.

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

9.10.2 Termination

9.10.3 Effect of termination and survival

9.11 Individual notices and communications with participants

The FPKIPA will be notified of any change in management or operational control of a CA.

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

In the event of a conflict between these Requirements and a law, regulation or government order (hereinafter 'Law') of any jurisdiction in which a CA operates or issues certificates, a CA MAY modify any conflicting requirement to the minimum extent necessary to make the requirement valid and legal in the jurisdiction. This applies only to operations or certificate issuances that are subject to that Law. In such event, the CA SHALL immediately (and prior to issuing a certificate under the modified requirement) include in Section 9.16.3 of the CA's CPS a detailed reference to the Law requiring a modification of these Requirements under this section, and the specific modification to these Requirements implemented by the CA.

The CA MUST also (prior to issuing a certificate under the modified requirement) notify the CA/Browser Forum of the relevant information newly added to its CPS by sending a message to questions@cabforum.org and receiving confirmation that it has been posted to the Public Mailing List and is indexed in the Public Mail Archives available at https://cabforum.org/pipermail/public/ (or such other email addresses and links as the Forum may designate), so that the CA/Browser Forum may consider possible revisions to these Requirements accordingly.

Any modification to CA practice enabled under this section MUST be discontinued if and when the Law no longer applies, or these Requirements are modified to make it possible to comply with both them and the Law simultaneously. An appropriate change in practice, modification to the CA's CPS and a notice to the CA/Browser Forum, as outlined above, MUST be made within 90 days.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

9.16.5 Force Majeure

9.17 Other provisions