DigiCert

Certificate Policy

DigiCert, Inc.
Version 4.12
September 8, 2017

2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481
www.digicert.com

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This Certificate Policy (CP) defines the procedural and operational requirements that DigiCert requires entities to adhere to when issuing and managing digitally signed objects (digital Certificates and time-stamp tokens) within DigiCert's PKI, excluding participants in DigiCert's Private PKI services, which are not cross-certified or publicly trusted. Specific requirements regarding those Certificates are set forth in the individual agreements with the appropriate DigiCert customer.

DigiCert's Certificate and time-stamp policies are controlled by the DigiCert Policy Authority (DCPA) that determines how this CP applies to Certificate Authorities (CAs), Registration Authorities (RAs), Subscribers, Relying Parties and other PKI entities that interoperate with or within the DigiCert PKI.

This document specifies the policies DigiCert adopts to meet the current versions of the following policies, guidelines, and requirements:

- the Federal Bridge Certification Authority ("FBCA") Certificate Policy,
- the Certification Authority / Browser Forum ("CAB Forum") Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements") located at https://cabforum.org/baseline-requirements-documents,
- the CAB Forum Guidelines for Extended Validation Certificates ("EV Guidelines") located at https://cabforum.org/extended-validation,
- the CAB Forum Guidelines for the Issuance and Management of Extended Validation Code Signing Certificates, and
- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates ("Minimum Requirements for Code Signing") located at https://aka.ms/csbr.

With regard to SSL/TLS Server Certificates or Code Signing Certificates, if any inconsistency exists between this CP and the requirements and guidelines above , then the requirements and guidelines above take precedence. Time-stamping policies are in accordance with IETF RFC 3161, X9.95, ETSI 102 023, and ETSI 101 861 technical standards.

Client Certificates follow the identity assurance frameworks found in the FBCA CP, NIST 800-63, the Kantara Initiative, and EU law applicable to Qualified Certificates.

This CP is only one of several documents that govern the DigiCert PKI. Other important documents include Certification Practice Statements, registration authority agreements and practice statements, subscriber agreements, relying party agreements, customer agreements, privacy policies, and memoranda of agreement. DigiCert may publish additional certificate policies or certification practice statements as necessary to describe other product and service offerings. These supplemental policies and statements are available to applicable users or relying parties.

Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP is divided into nine parts that cover the security controls and practices and procedures for certificate or time-stamping services within the DigiCert PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certificate Policy and was approved for publication on 2 August 2010 by the DigiCert Policy Authority (DCPA). The following revisions have been made to the original document:

Date	Changes	Version
8-September-2017	Removed references to PIV-I throughout, conflicts of interest	4.12

Date	Changes	Version
	in section 5.2.1, auditor qualifications in section 8.2, and made other minor changes.	
23-February-2017	Updated address, made revisions related to the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and made other changes to update the CP.	4.11
9-September-2016	Updated to clarify ID documents allowed and for consistency with FBCA CP 2.29, and sec. 9.6.3 of Baseline Requirements	4.10
1-June-2015	Updated for consistency with CA/Browser Forum Baseline Requirements and new Federal PIV-I Profile reference	4.09
1-April-2015	Made additional changes based on FPKI CPWG review.	4.08
7-October-2014	Updated for consistency with FBCA CP v. 2.27	4.07
14-May-2014	Updated to comply with changes to Baseline Requirements and the EV Guidelines.	4.06
2-May-2013	Updated mailing address, removed references to Adobe CDS Program, revised explanation of Level 2 identification requirements, revised private key management provisions and key ceremony witness requirements.	4.05
10-May-2012	Updated to include provisions set forth in the Baseline Requirements, to add EV Code Signing, improve readability, and to modify requirements related to IGTF Certificates.	4.04
3-May-2011	Policy OIDs revised for certain certificate types and minor updates made to various sections.	4.03
29-October-2010	Changes made in response to comments from the FPKI CPWG regarding certificate status services, trusted roles, and off-site backup of archive.	4.02
26-August-2010	Updated the process used to authenticate the certificate requester's authority under section 3.2.5 for code signing certificates issued to organizations	4.01
2-August-2010	This version 4.0 replaces the DigiCert Certificate Policy and Certification Practices Statement, Version 3.08, dated May 29, 2009.	4.0

The OID for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412). DigiCert organizes its OID arcs for the various Certificates and documents described in this CP as follows:

Digitally Signed Object	**Object Identifier (OID)**
Policy Documents	2.16.840.1.114412.0
This CP Document	2.16.840.1.114412.0.1.4
Certificates issued pursuant to CPS	2.16.840.1.114412.0.2.4
Non EV SSL/TLS Server Certificates	2.16.840.1.114412.1
Organization-Validated SSL/TLS Certificate*	2.16.840.1.114412.1.1
Domain-Validated SSL/TLS Certificate*	2.16.840.1.114412.1.2
Hotspot 2.0 OSU Server Certificates	2.16.840.1.114412.1.5
Federated Device Certificate	2.16.840.1.114412.1.11
Federated Device Hardware Certificate	2.16.840.1.114412.1.12
Extended Validation SSL/TLS Certificates *	2.16.840.1.114412.2
Object Signing Certificates	2.16.840.1.114412.3
Code Signing	2.16.840.1.114412.3.1
Minimum Requirements for Code Signing	2.16.840.1.114412.3.1.1
Extended Validation Code Signing*	2.16.840.1.114412.3.2
Windows Kernel Driver Signing	2.16.840.1.114412.3.11

Adobe Signing Certificates	2.16.840.1.114412.3.21
Client Certificate OID arc	2.16.840.1.114412.4.
Level 1 Certificates – Personal	2.16.840.1.114412.4.1.1
Level 1 Certificates – Enterprise	2.16.840.1.114412.4.1.2
Level 2 Certificates	2.16.840.1.114412.4.2
Level 3 Certificates – US	2.16.840.1.114412.4.3.1
Level 3 Certificates – CBP	2.16.840.1.114412.4.3.2
Level 4 Certificates – US	2.16.840.1.114412.4.4.1
Level 4 Certificates – CBP	2.16.840.1.114412.4.4.2
Grid Certificates	2.16.840.1.114412.4.31 or 2.16.840.1.114412.31 (Grid-only arc)
IGTF-Comparable to Classic with Secured Infrastructure	2.16.840.1.114412.4.31.1 (Client w/ Public) or 2.16.840.1.114412.31.4.1.1 (Client Grid Only)
IGTF-Comparable to Member-Integrated Credential Services with Secured Infrastructure	2.16.840.1.114412.4.31.5
IGTF Grid Host - Public Trust	2.16.840.1.114412.1.31.1
Grid-Only Host Certificate	2.16.840.1.114412.31.1.1.1
Authentication-Only Certificates	2.16.840.1.114412.6
Legacy arc	2.16.840.1.114412.81
Test arc	2.16.840.1.114412.99

* Also governed by guidelines of the CA/Browser Forum.

This CP applies to any entity asserting one or more of the DigiCert OIDs identified above. When a CA issues a Certificate containing one of the above-specified policy identifiers, it asserts that the Certificate was issued and is managed in accordance with the requirements applicable to that respective policy. All other OIDs mentioned above belong to their respective owners. Commercial Best Practices ("CBP") differs from "US" in that there are no trusted role citizenship requirements for an Issuer CA issuing under a CBP policy, whereas policies designated "US" must follow the citizenship practices set forth in Section 5.3.1 of this CP.

The Legacy arc exists to identify Certificates issued for purpose of achieving compatibility with legacy systems that are incapable of processing newer algorithms that might be required by comparable industry best practices.

Subsequent revisions to this CP might contain new OID assignments for the certificate types identified above.

1.3. PKI PARTICIPANTS

1.3.1. DigiCert Policy Authority and Certification Authorities

DigiCert Root Certificate Authorities and Intermediate CAs are managed by the DigiCert Policy Authority (DCPA) which is composed of members of DigiCert management appointed by DigiCert's executive management. The DCPA is responsible for this CP, the approval of related practice statements, and overseeing the conformance of CA practices with this CP. DigiCert's policies are designed to ensure that the DigiCert PKI complies, in all material respects, with U.S. and international standards and regulations, including the Federal Bridge Certificate Policy, EU law, CA/Browser Forum Guidelines, and relevant law on electronic signatures. DigiCert may establish or recognize other CAs (e.g. subordinate CAs) in accordance with this CP, applicable cross-certification / federation policies and memoranda of agreement. For ease of reference herein, all CAs issuing Certificates in accordance with this CP (including DigiCert) are hereafter referred to as "Issuer CAs."

DigiCert shall notify the U.S. Federal PKI Policy Authority (FPKIPA) prior to issuing any CA Certificate to an external Issuer CA that DigiCert desires to chain to the Federal Bridge CA.

1.3.2. Registration Authorities

Registration Authorities (RA) operate identity management systems (IdMs) and collect and verify Subscriber information on the Issuer CA's behalf. The requirements in this CP apply to all RAs. An Issuer CA shall monitor each RA's compliance with this policy, the CPS, and if applicable, any Registration Practices Statement (RPS) under which the RA operates. An Issuer CA that relies on a variety of RAs or IdMs to support various communities of interest may submit an RPS for each RA or IdM to the DCPA for approval. The RPS must contain details necessary for the DCPA to determine how the RA achieves compliance with this Policy. Necessary details include how the RA's process or IdM establishes the identities of applicants, how the integrity and authenticity of such identifying information is securely maintained and managed, and how changes and updates to such information are communicated to the Issuer CA.

1.3.3. Subscribers

Subscribers use DigiCert's services and PKI to support transactions and communications. Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the Certificate. A *Subscriber*, as used herein, refers to both the subject of the Certificate and the entity that contracted with the Issuer CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by the Issuer CA. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate.

1.3.5. Other Participants

Other participants include Bridge CAs and CAs that cross-certify Issuer CAs to provide trust among other PKI communities.

1.4. CERTIFICATE USAGE

A *digital Certificate* (or C*ertificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.
A *time-stamp token* (*TST*) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

1.4.1. Appropriate Certificate Uses

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CP.

1.4.2. Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued. Code signing Certificates do not indicate that the signed code is safe to install or is free from malware, bugs, or vulnerabilities.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CP and the documents referenced herein are maintained by the DCPA, which can be contacted at:

DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
Tel: 1-801-701-9600
Fax: 1-801-705-0481
www.digicert.com
support@digicert.com

1.5.2. Contact Person

Attn: Legal Counsel
DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
www.digicert.com
support@digicert.com

1.5.3. Person Determining CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CP and the conformance of a CPS to this CP based on the results and recommendations received from an independent auditor (see Section 8). The DCPA is also responsible for evaluating and acting upon the results of compliance audits.

1.5.4. CP Approval Procedures

The DCPA approves the CP and any amendments. Amendments are made by either updating the entire CP or by publishing an addendum. The DCPA determines whether an amendment to this CP requires notice or an OID change. *See also* Section 9.10 and Section 9.12 below.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

"Affiliated Organization" means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a Certificate.

"Applicant" means an entity applying for a certificate.

"Certificate" means an electronic document that uses a digital signature to bind a Public Key and an identity.

"EV Guidelines" is defined in section 1.1.

"Key Pair" means a Private Key and its associated Public Key.

"OCSP Responder" means an online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.

"Private Key" means 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" means 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.

"Qualified Certificate" means a Certificate that meets the requirements of EU law and is provided by an Issuer CA meeting the requirements of EU law.

"Relying Party" means an entity that relies upon either the information contained within a Certificate or a time-stamp token.

"Relying Party Agreement" means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert's Repository.

"Secure Signature Creation Device" means a signature-creation device that meets the requirements laid down in EU law.

"Subscriber" means either the entity identified as the subject in the Certificate or the entity receiving DigiCert's time-stamping services.

"**Subscriber Agreement"** means an agreement that governs the issuance and use of a Certificate that the Applicant must read and accept before receiving a Certificate.

"WebTrust" means the current version of CPA Canada's WebTrust Program for Certification Authorities.

1.6.2. Acronyms

CA	Certificate Authority or Certification Authority
CBP	Commercial Best Practices
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCPA	DigiCert Policy Authority
DV	Domain Validated
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector

MICS	Member-Integrated Credential Service (IGTF)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PIN	Personal Identification Number (e.g. a secret access code)
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

CA/Browser Forum Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates ("Baseline Requirements")

CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates ("EV Guidelines")

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

Issuer CAs shall publish all publicly trusted CA Certificates and cross-Certificates, issued to and from the Issuer CA, revocation data for issued digital Certificates, CP, CPS, and standard Relying Party Agreements and Subscriber Agreements in online repositories. The Issuer CA shall ensure that its root Certificate and the revocation data for issued Certificates are available through a repository 24 hours a day, 7 days a week with a minimum of 99% availability overall per year with a scheduled down-time that does not exceed 0.5% annually.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

Issuer CAs shall make the following information publicly accessible on the web: all publicly trusted root Certificates, cross Certificates, CRLs, CPs and CPSs. Pointers to repository information in CA and end entity Certificates shall only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties.

2.3. TIME OR FREQUENCY OF PUBLICATION

Issuer CAs shall publish CA Certificates and revocation data as soon as possible after issuance. Issuer CAs shall publish new or modified versions CPSs within seven days of their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

Information published in a repository is public information. The Issuer CA shall provide unrestricted read access to its repositories and shall implement logical and physical controls to prevent unauthorized write access to such repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Issuer CAs shall issue Certificates with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. Level 1 Certificates may include a null subject DN if they include at least one alternative name form that is marked critical. Subject Alternate Name forms may be included in Certificates if they are marked non-critical. When DNs are used, common names must respect name space uniqueness and must not be misleading.

Issuer CAs shall comply with section 3.1.2 of RFC 3739 when providing EU Qualified Certificates.

3.1.2. Need for Names to be Meaningful

When applicable, Issuer CAs shall use distinguished names to identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. Directory information trees shall accurately reflect organizational structures.

When applicable, Issuer CAs shall ensure that each User Principal Name (UPN) is unique and accurately reflects organizational structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Issuer CAs may issue end-entity anonymous or pseudonymous Certificates provided that (i) such Certificates are not prohibited by applicable policy (e.g. for certificate type, assurance level, or certificate profile) and (ii) name space uniqueness is preserved.

3.1.4. Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using X.500 standards and ASN.1 syntax. *See* RFC 2253 and RFC 2616 for further information on how X.500 distinguished names in Certificates are interpreted as Uniform Resource Identifiers and HTTP references.

3.1.5. Uniqueness of Names

The DCPA shall enforce name uniqueness in Certificates that are trusted within the DigiCert PKI. The DCPA may enforce uniqueness by requiring that each Certificate include a unique serial number that is incorporated as part of the subject name.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with any content that infringes the intellectual property rights of another entity. Unless otherwise specifically stated, this CP does not require an Issuer CA to verify an Applicant's right to use a trademark. Issuer CAs may reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2. INITIAL IDENTITY VALIDATION

An Issuer CA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The Issuer CA may refuse to issue a Certificate in its sole discretion.

3.2.1. Method to Prove Possession of Private Key

The Issuer CA shall verify that the Applicant possesses the Private Key corresponding to the Public Key in the certificate request. The Issuer CA shall require that Private Keys for EU Qualified Certificate be generated in the Subscriber's presence on a Secure Signature Creation Device (SSCD) (OID 0.4.0.1456.1.1) and stored securely on the SSCD with a Subscriber-selected PIN.

3.2.2. Authentication of Organization and Domain Identity

Domain names included in a publicly trusted SSL/TLS Certificate must be verified in accordance with Section 3.2.2.4 of the Baseline Requirements.

If a publicly-trusted SSL/TLS Certificate will contain an organization's name, then the Issuer CA (or an RA) shall verify the information about the organization and its legal existence in accordance with Section 3.2.2.1 of the Baseline Requirements using reliable third party and government databases or through other direct means of communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition.

If the request is for a Certificate that asserts an organizational affiliation between a human subscriber and an organization, the Issuer CA shall obtain documentation from the organization that recognizes the affiliation and obligates the organization to request revocation of the Certificate if that affiliation ends. See Sections 3.2.5, 4.9.1 and 9.6.1.

Issuer CAs and RAs shall identify high-risk certificate requests and shall conduct additional verification activity and take additional precautions as are reasonably necessary to ensure that high-risk requests are properly verified.

All requests for Issuer CA Certificates or Certificates with an organization's name that are cross-certified with the FBCA shall include the organization name, address, and documentation of the existence of the organization. For Issuer CA Certificates and CA cross-Certificates, representatives of the DCPA verify the information, in addition to the authenticity of the requesting representative and the representative's authorization for the Certificate.

3.2.3. Authentication of Individual Identity

The Issuer CA or an RA shall verify an individual's identity in accordance with the process established in its CPS or RPS that meets the following minimum requirements:

Certificate	Identity Verification
SSL/TLS Server Certificates and Object Signing Certificates (issued to an Individual)	The Applicant shall submit a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The copy of the document shall be inspected for any indication of alteration or falsification. If the Issuer CA or RA requires further assurance, the Applicant shall provide additional forms of identification, including non-photo and non-governmental forms of identification such as recent utility bills, financial account statements, Applicant credit card, additional ID credential, or equivalent document type. The Issuer CA or RA shall confirm that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If the Issuer CA or RA cannot verify the Applicant's identity using the procedures described above, then the Issuer CA or RA shall obtain a Declaration of Identity* witnessed and signed by a Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Device Certificate Sponsors	See section 3.2.3.3
EV SSL/TLS Certificates	As specified in the EV Guidelines

issued to a Business Entity	
Authentication-Only Certificates	The entity controlling the secure location represents that the certificate holder has authorization to access the location.
Grid-only Certificates	Either the RA responsible for the grid community or a Trusted Agent must either review an identity document during a face-to-face meeting with the Applicant, or a Trusted Agent must attest that the Applicant is personally known to the Trusted Agent. If an identification document is used, the RA must retain sufficient information about the Applicant's identity in order to verify the Applicant at a later date.
Level 1 Client Certificates – Personal (email certificates)	Applicant's control over an email address (or any of the identity verification methods listed for a higher level client certificate).
Level 1 Client Certificates - Enterprise (email certificates)	Any one of the following: 1. In-person appearance before an RA or Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: - the ability to place or receive calls from a given number; or - the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: - the ability to obtain mail at the billing address used in the business relationship; or - verification of information established in previous transactions (e.g., previous order number); or - the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method required to verify identity for issuance of a Level 2, 3, or 4 Client Certificate
Level 2 Client Certificates	This level of assurance requires that the Issuer CA or RA verify the Applicant's identity using the possession of a reliable form of identification. Personal identifying information shall be compared with Applicant-provided information to confirm that the asserted name matches: (a) the name contained in the presented identification credential; (b) the individual's date of birth; and (c) a current address or personal telephone number sufficient to identify a unique individual. The Issuer CA or RA shall verify the Applicant's identity using one of the following four (4) methods: 1. In-person proofing before an RA or Trusted Agent (or entity certified by a State or National Government as authorized to confirm identities) with presentment of a valid current government-issued

	identity document that contains the Applicant's picture and either address of record or nationality (e.g. driver's license or Passport). Such authentication does not relieve the RA of its responsibility to verify the presented data. 2. Remotely verifying information provided by the Applicant (verified electronically by a record check with the specified issuing authority or through similar databases to establish the existence of such records with matching name and reference numbers and to corroborate date of birth and current address of record or telephone number). The Issuer CA or RA may confirm an address by issuing the credentials in a manner that confirms the address of record or verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records that are available to the Issuer CA or RA. 3. If the Issuer CA or RA has a current, ongoing relationship with the Applicant, the Issuer CA or RA may verify identity using an exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo ID, and (b) the ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods required to verify identity for issuance of a DigiCert Level 3 or 4 Client Certificate.
Level 3 Client Certificates	In-person proofing before an RA, Trusted Agent, or an entity certified by a State or National Government that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). The Applicant shall provide at least one Federal Government-issued Picture I.D., a REAL ID, or two Non-Federal Government I.D.s, one of which must be a photo I.D. Acceptable forms of Non-Federal Government photo IDs include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See USCIS Form I-9. The Issuer CA or RA shall examine the credentials and determine whether they are authentic and unexpired. For each Level 3 or higher assurance Client Certificate issued, the Issuer CA or the RA shall review and record a Declaration of Identity* which shall be signed by the applicant and the person performing the in-person identification. The Issuer CA or RA shall check the provided information (name, date

	of birth, and current address) to ensure legitimacy and may verify it electronically by a record check as described above. The Issuer CA or RA may employ an in-person antecedent process, defined in FBCA Supplementary Antecedent, In-Person Definition, to meet the in-person identity proofing requirement. Under this definition, historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, the Applicant (e.g. an employee) has been identified previously by an employer using USCIS Form I-9 and is bound to the asserted identity remotely through the use of known attributes or shared secrets. In another use case, a third party Identity Verification Provider constructs a real-time, five-question process, based on multiple historic antecedent databases, and the applicant is given two minutes to answer at least four of the five questions correctly. See FBCA Supplementary Antecedent, In-Person Definition. If the photo ID is unexpired and confirms the address of record for the Applicant, then the certificate may be approved for issuance with notice of issuance sent to the address of record. If the photo ID does not confirm the Applicant's address of record, then the certificate shall be issued in a manner that confirms the address of record. For all Level 3 or higher assurance Client Certificates, the identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.
Level 4 Client Certificates (Medium Hardware) Must be issued to cryptographic hardware.	In-person proofing before an RA, Trusted Agent, or an entity certified by a State or National Government that is authorized to confirm identities (provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner and that the RA is not relieved of its responsibility to verify the presented data). The Application shall supply (i) one Federal Government-issued Picture I.D., a REAL ID, or two Non-Federal Government I.D.s, one of which must be a photo I.D. and (ii) the contemporaneous collection of at least one biometric (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application. Acceptable forms of Non-Federal Government photo IDs include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See USCIS Form I-9. The Issuer CA or RA shall examine the credentials and determine whether they are authentic and unexpired. For each Level 4 Client Certificate issued, the Issuer CA or the RA shall review and record a Declaration of Identity* that is signed by the applicant and the person performing the in-person identification. For all Level 4 Client Certificates the use of an in-person antecedent is not applicable and the Applicant shall establish his or her identity no

	more than 30 days prior to initial certificate issuance. Issuer CAs and RAs shall issue Level 4 Client Certificates in a manner that confirms the Applicant's address of record.
EU Qualified Certificates	In-person verification of the Applicant's identity by appropriate means in accordance with national law. The entity performing the validation shall check the evidence of identity directly against a physical person or indirectly using means that provide equivalent assurance to physical presence.

* A Declaration of Identity consists of the following:
    a. the identity of the person performing the verification;
    b. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law; the signature on the declaration may be either a handwritten or digital signature using a certificate that is of equal or higher level of assurance as the credential being issued;
    c. unique identifying number(s) from the Applicant's identification document(s), or a facsimile of the ID(s);
    d. the date of the verification; and
    e. a declaration of identity by the Applicant that is signed (in handwriting or through use of a digital signature that is of equivalent or higher assurance than the credential being issued) in the presence of the person performing the verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

Where in-person identity verification is required and the Applicant cannot participate in face-to-face registration alone (e.g. because Applicant is a network device, minor, or person not legally competent), then the Applicant may be accompanied by a person already certified by the PKI or who has the required identity credentials for a Certificate at the same or higher level of assurance applied for by the Applicant. The person accompanying the Applicant (i.e. the "Sponsor") will present information sufficient for registration at the level of the certificate being requested, for himself or herself, and for the Applicant.

For in-person identity proofing at Levels 3 and 4, an entity certified by a State or National Government as authorized to confirm identities may perform in-person authentication on behalf of the RA. The information collected from the applicant should be reliably collected from the certified entity. Packages secured in a tamper-evident manner by the certified entity satisfy this requirement; other secure methods are also acceptable. Such authentication does not relieve the RA of its responsibility to verify the presented data.

3.2.3.1. Authentication for Role-based Client Certificates

An Issuer CA may issue Certificates that identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). These role-based Certificates are used when non-repudiation is desired. The Issuer CA may only issue role-based certificates to Subscribers who first obtain an individual Subscriber Certificate that is at the same or higher assurance level as the requested role-based Certificate. An Issuer CA may issue Certificates with the same role to multiple Subscribers. However, the Issuer CA shall require that each Certificate have a unique Key Pair. Individuals may not share their issued role-based Certificates and are required to protect the role-based Certificate in the same manner as individual Certificates.

The Issuer CA or an RA shall verify the identity of the individual requesting a role-based Certificate (i.e. the sponsor) in accordance with Section 3.2.3 and record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role-based Certificate. The sponsor must hold an individual Certificate in his/her own name issued by the same CA at the same or higher assurance level as the role-based Certificate.

Procedures and policies for issuing role-based Certificates shall comply with all provisions of this CP (e.g., key generation, private key protection, and Subscriber obligations).

IGTF and EU Qualified Certificates are not issued as role-based Certificates.

If the Certificate is a pseudonymous certificate cross-certified with the FBCA that identifies subjects by their organizational roles, then the Issuer CA or RA shall verify that the individual either holds that role or has the authority to sign on behalf of the role.

3.2.3.2. Authentication for Group Client Certificates

If several entities are acting in one capacity and non-repudiation is not necessary, the Issuer CA may issue a Certificate corresponding to a Private Key shared by multiple Subscribers. The Issuer CA or RA shall record the information identified in Section 3.2.3 for a sponsor from the Information Systems Security Office or equivalent before issuing a group Certificate.

In addition, the Issuer CA or the RA shall:

1. Require that the Information Systems Security Office, or equivalent, be responsible for ensuring control of the Private Key, including maintaining a list of Subscribers who have access to the Private Key, and account for the time period during which each Subscriber had control of the key,
2. Not include a subjectName DN in the certificate in a way that could imply that the subject is a single individual ,
3. Require that the sponsor provide and continuously update a list of individuals who hold the shared Private Key, and
4. Ensure that the procedures for issuing group certificates comply with all other stipulations of this CP (e.g., key generation, private key protection, and Subscriber obligations).

IGTF and EU Qualified Certificates are not issued as group Certificates.

3.2.3.3. Authentication of Devices with Human Sponsors

An Issuer CA may issue a Level 1, 2, 3 or 4 Client or Federated Device Certificate for use on a computing or network device, provided that the entity owning the device is listed as the subject. In such cases, the device must have a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment Public Keys,
3. Equipment authorizations and attributes (if any are to be included in the certificate), and
4. Contact information.

If the Certificate's sponsor changes, the new sponsor shall review the status of each device to ensure it is still authorized to receive Certificates. The CPS shall describe procedures to ensure that certificate accountability is maintained.

The Issuer CA shall verify all registration information commensurate with the requested certificate type. Acceptable methods for performing this authentication and integrity checking include:

1. Verification of digitally signed messages sent from the sponsor (using Certificates of equivalent or greater assurance than that being requested)
2. In person registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.

3.2.4. Non-verified Subscriber Information

Issuer CAs are not required to confirm that the common name in a Level 1 - Personal Client Certificate is the legal name of the Subscriber. Any other non-verified information included in a Certificate shall be designated as such in the Certificate. No unverified information shall be

included in any Level 2, Level, 3, Level 4, Object Signing, EV, Federated Device, or EU Qualified Certificate.

3.2.5. Validation of Authority

The Issuer CA or RA shall verify the authorization of a certificate request as follows:

Certificate	Verification
DV SSL/TLS Certificates, OV SSL/TLS Certificates, and Federated Device Certificates	An authorized contact listed with the Domain Name Registrar, a person with control over the domain name, or through communication with the applicant using a Reliable Method of Communication, as defined in the Baseline Requirements.
EV Certificates	In accordance with the EV Guidelines.
Object Signing Certificates (including EV Code Signing Certificates)	If a Certificate names an organization, an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a Reliable Method of Communication.
Level 1 Client Certificates - Personal or Enterprise (email certificates)	An individual with control over the email address listed in the Certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the Certificate.
IGTF Certificates	Pursuant to the relevant requirements by the accreditation authority.
Client Certificates Levels 2, 3 and 4	Individuals affiliated with the organization who confirm the applicant's authority to obtain a Certificate indicating the affiliation and who agree to request revocation of the Certificate when that affiliation ends.
EU Qualified Certificates	An individual is associated with the organization that is authorized to consent to the Certificate's publication (see section 7.3.1 of TS 101 456).

The Issuer CA shall implement a process whereby an Applicant may limit the number of individuals authorized to request Certificates. The Issuer CA shall provide a list of authorized certificate requesters after receiving a verified request for such information from an individual authorized to make such request.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

An Issuer CA may allow Subscribers of SSL/TLS Server and Code Signing Certificates to authenticate themselves over a TLS/SSL session with username and password. Each Subscriber shall reestablish its identity using the initial registration processes of section 3.2 according to the following table:

Certificate	Routine Re-Key Authentication	Re-Verification Required
DV and OV SSL/TLS Certificates	Username and password	
EV SSL/TLS Certificates	Username and password	According to the EV Guidelines
Subscriber Code Signing Certificates (Minimum Requirements and EV)	Username and password	At least every 39 months
Signing Authority EV Code Signing Certificates	Username and password	At least every 123 months
Timestamp EV Code Signing Certificates	Username and password	At least every 123 months
Object Signing Certificates	Username and password	At least every six years
Level 1 Client Certificates	Username and password	At least every nine years
Level 2 Client Certificates	Current signature key or multi-	At least every nine years

	factor authentication meeting NIST SP 800-63 Level 3	
Level 3 and 4 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Federated Device and Federated Device-hardware	Current signature key or multi-factor authentication meeting NIST-800-63 Level 3	At least every nine years
IGTF Certificates	Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated Private Key	At least every 13 months. However, certificates associated with a Private Key restricted solely to a hardware token may be rekeyed or renewed for a period of up to 5 years
Authentication-Only Certificates	Username and password or with associated Private Key	None

The Issuer CA shall not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

The Issuer CA shall require subscribers of Certificates that have been revoked for reasons other than as the result of a routine certificate renewal, update, or modification action to undergo the initial registration process (described in Section 3.2) to obtain a new Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

The Issuer CA or the RA that approved the Certificate's issuance shall authenticate all revocation requests. The Issuer CA or RA may authenticate a revocation request using the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

No individual or entity listed on a government denied list, list of prohibited persons, or other list that prohibits doing business with such organization or person under the laws of the United States may submit an application for a Certificate.

4.1.2. Enrollment Process and Responsibilities

The Issuer CA is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CP and the applicable CPS prior to the issuance of a Certificate. Applicants are responsible for submitting sufficient information and documentation for the Issuer CA or the RA to perform the required verification of identity prior to issuing a Certificate.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

The Issuer CA or the RA shall identify and verify each Applicant in accordance with the applicable Certification Practice Statements and Registration Practice Statements. The Issuer CA shall ensure that all communication between the Issuer CA and an RA regarding certificate issuance or changes in the status of a Certificate are made using secure and auditable methods. If databases or other sources are used to confirm sensitive or confidential attributes of an individual subscriber, then that

sensitive information shall be protected and securely exchanged in a confidential and tamper-evident manner, protected from unauthorized access, and tracked using an auditable chain of custody.

4.2.2. Approval or Rejection of Certificate Applications

The Issuer CA shall reject any certificate application that cannot be verified. The Issuer CA may also reject a certificate application on any reasonable basis, including if the Certificate could damage the Issuer CA's business or reputation. Issuer CAs are not required to provide a reason for rejecting a certificate application.

Issuer CAs and RAs shall follow industry standards when approving and issuing Certificates. The Issuer CA or RA shall contractually require subscribers to verify the information in a Certificate prior to using the Certificate.

4.2.3. Time to Process Certificate Applications

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. Identity shall be established no more than 30 days before initial issuance of Level 3 and 4 Certificates.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

Issuer CAs shall verify the source of a certificate request before issuance. The Issuer CA and any RA shall protect databases under their control and that are used to confirm Subscriber identity information from unauthorized modification or use. The Issuer CA shall perform its actions during the certificate issuance process in a secure manner.

4.3.2. Notification to Subscriber by the CA of Issuance of Certificate

The Issuer CA or RA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

The passage of time after delivery or notice of issuance of a Certificate to the Subscriber or the actual use of a Certificate constitutes the Subscriber's acceptance of the Certificate.

4.4.2. Publication of the Certificate by the CA

The Issuer CA shall publish all CA Certificates to the Issuer CA's repository.

4.4.3. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

All Subscribers shall protect their Private Keys from unauthorized use or disclosure by third parties and shall use their Private Keys only for their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties shall use software that is compliant with X.509 and applicable IETF PKIX standards. The Issuer CA shall specify restrictions on the use of a Certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP). Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. Relying on a digital signature or Certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

An Issuer CA may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the associated Private Key has not been compromised,
3. the Subscriber and attributes remain consistent, and
4. re-verification of subscriber identity is not required by Section 3.3.1.

An Issuer CA may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services. After renewing a client Certificate, the Issuer CA may not re-key, renew, or modify the old Certificate.

4.6.2. Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates. For Certificates cross-certified with the FBCA, renewal requests are only accepted from certificate subjects, PKI sponsors or RAs. An Issuer CA may perform renewal of its subscriber Certificates without a corresponding request, such as when the CA re-keys.

4.6.3. Processing Certificate Renewal Requests

The Issuer CA may require reconfirmation or verification of the information in a Certificate prior to renewal.

4.6.4. Notification of New Certificate Issuance to Subscriber

The Issuer CA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

The passage of time after delivery or notice of issuance of the Certificate to the Subscriber, or actual use of the Certificate, constitutes the Subscriber's acceptance of it.

4.6.6. Publication of the Renewal Certificate by the CA

The Issuer CA shall publish all renewed CA Certificates to the Issuer CA's repository.

4.6.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a Certificate consists of creating a new Certificate with a different Public Key (and serial number) while retaining the remaining contents of the old Certificate that describe the subject. The new Certificate may have a different validity period, key identifiers, specify different CRL and OCSP distribution points, and/or be signed with a different key.

Subscribers requesting re-key should identify and authenticate themselves as permitted by Section 3.3.1.

After re-keying a Client Certificate or a federated device Certificate, the Issuer CA may not re-key, renew, or modify the previous Certificate.

4.7.2. Who May Request Certificate Rekey

Only the subject of the Certificate or the PKI sponsor may request re-key. The Issuer CA or an RA may initiate certificate re-key at the request of the certificate subject or in its own discretion.

4.7.3. Processing Certificate Rekey Requests

Re-key requests are only accepted from the subject of the Certificate or the PKI sponsor. At a minimum, the Issuer CA shall comply with section 3.3.1 in identifying and authenticating the Subscriber or PKI sponsor prior to rekeying the Certificate.

4.7.4. Notification of Certificate Rekey to Subscriber

The Issuer CA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

The passage of time after delivery or notice of issuance of the Certificate to the Subscriber or the actual use of the Certificate constitutes the Subscriber's acceptance of it.

4.7.6. Publication of the Rekeyed Certificate by the CA

The Issuer CA shall publish rekeyed CA Certificates to the Issuer CA's repository.

4.7.7. Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstance for Certificate Modification

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CP. The new Certificate may have the same or a different subject Public Key. After modifying a Certificate that is cross-certified with the FBCA, the Issuer CA may not re-key, renew, or modify the old Certificate.

4.8.2. Who May Request Certificate Modification

The Issuer CA may modify a Certificate at the request of the certificate subject or in its own discretion.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, the Issuer CA shall verify any information that will change in the modified Certificate. The Issuer CA may issue the modified Certificate only after completing the verification process on all modified information. The validity period of a modified Certificate must not extend beyond the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4. Notification of Certificate Modification to Subscriber

The Issuer CA shall notify the Subscriber within a reasonable time of certificate issuance and may use any reliable mechanism to deliver the Certificate to the Subscriber.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

The passage of time after delivery or notice of issuance of the Certificate to the Subscriber or actual use of the Certificate constitutes the Subscriber's acceptance of it.

4.8.6. Publication of the Modified Certificate by the CA

The Issuer CA shall publish modified CA Certificates to the Issuer CA's repository.

4.8.7. Notification of Certificate Modification by the CA to Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, the Issuer CA shall verify that the revocation request was made by either the organization or individual that made the certificate application or by an entity with the legal jurisdiction and authority to request revocation. The Issuer CA should revoke a Certificate if the Issuer CA is aware that:

1. The Subscriber requested revocation of its Certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised or misused;
4. The Subscriber or the cross-certified CA breached a material obligation under the CP, the CPS, or the relevant agreement;
5. Either the Subscriber's or the Issuer CA's obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The Applicant has lost its rights to a trademark or the domain name listed in the Certificate;
7. The Certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
8. The Issuer CA received a lawful and binding order from a government or regulatory body to revoke the Certificate;
9. The Issuer CA ceased operations and did not arrange for another certificate authority to provide revocation support for the Certificate;
10. The Issuer CA's right to manage Certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and to maintain the CRL/OCSP Repository);
11. Any information appearing in the Certificate was or became inaccurate or misleading;
12. The technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others;
13. The Subscriber was added as a denied party or prohibited person to a blacklist, or is operating from a destination prohibited under U.S. law; or
14. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware or other harmful content, including any code that is downloaded onto a user's system without their consent.

The Issuer CA shall revoke a Certificate if the binding between the subject and the subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

If a Certificate expresses an organizational affiliation, the Issuer CA or the RA shall require the Affiliated Organization to inform it if the subscriber affiliation changes. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, then the Issuer CA shall revoke any Certificates

issued to that Subscriber containing the organizational affiliation. If an Affiliated Organization terminates its relationship with the Issuer CA or RA such that it no longer provides affiliation information, the Issuer CA shall revoke all Certificates affiliated with that Affiliated Organization.

An Issuer CA or cross-certified entity shall request revocation of its DigiCert-issued cross-Certificate if it no longer meets the stipulations of DigiCert's policies, as indicated by DigiCert's policy OIDs in Certificates or those listed in the policy mapping extension of the cross-Certificate.

4.9.2. Who Can Request Revocation

The Issuer CA or RA shall accept revocation requests from authenticated and authorized parties, such as the certificate Subscriber or the Affiliated Organization named in a Certificate. The Issuer CA or RA may establish procedures that allow other entities to request certificate revocation for fraud or misuse. The Issuer CA shall revoke a Certificate if it receives sufficient evidence of compromise of loss of the Private Key. The Issuer CA may revoke a Certificate of its own volition without reason, even if no other entity has requested revocation.

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. The Issuer CA or RA shall authenticate and log each revocation request. The Issuer CA will always revoke a Certificate if the request is authenticated as originating from the Subscriber or the Affiliated Organization listed in the Certificate. If revocation is requested by someone other than an authorized representative of the Subscriber or Affiliated Organization, the Issuer CA or RA shall investigate the alleged basis for the revocation request.

The Issuer CA shall maintain a continuous 24/7 ability to internally respond to any high priority certificate problem reports. If appropriate, the Issuer CA or the RA may forward complaints to law enforcement.

4.9.4. Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber must make a revocation request after reasons for revocation have been identified. Issuer CAs and RAs are required to report the suspected compromise of their CA or RA Private Key and request revocation to both the policy authority and operating authority of the superior issuing CA (e.g., the FPKIPA/FBCA OA, DCPA, cross-signing CA, Root CA, etc.) within one hour of discovery. Subscribers shall request revocation as soon as possible if the Private Key corresponding to the Certificate is lost or compromised or if the certificate data is no longer valid. The Issuer CA may extend revocation grace periods on a case-by-case basis.

4.9.5. Time within which CA Must Process the Revocation Request

An Issuer CA shall revoke a Certificate within one hour of receiving appropriate instruction from the DCPA. An Issuer CA shall revoke the CA Certificate of a subordinate or cross-signed CA as soon as practical after receiving proper notice that the subordinate or cross-signed CA has been compromised. If an Issuer CA or the DCPA determines that immediate revocation is not practical, because the potential risks of revocation outweigh the risks caused by the compromise, then the Issuer CA and the DCPA shall jointly determine the appropriate process to follow in order to promptly revoke the subordinate or cross-signed CA Certificate.

The Issuer CA shall revoke other Certificates as quickly as practical after validating the revocation request. The Issuer CA shall process revocation requests as follows:

1. Before the next CRL is published, if the request is received two or more hours before regular periodic CRL issuance,
2. By publishing it in the CRL following the next CRL, if the request is received within two hours of the regularly scheduled next CRL issuance, and
3. Regardless, within 18 hours after receipt.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on the information listed in a Certificate, a Relying Party shall confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain.

4.9.7. CRL Issuance Frequency

CRL issuance is comprised of CRL generation and publication. For Issuer CAs and online intermediate CAs, the interval between CRL issuance shall not exceed 24 hours. For Root CAs and Intermediate CAs that are operated in an off-line manner, routine CRLs may be issued less frequently than specified above, provided that the CA only issues CA Certificates, certificate-status-checking Certificates, and internal administrative Certificates. CRL issuance intervals for such offline CAs are no greater than 6 months. However, the interval between routine CRL issuance for offline CAs chaining to the Federal Bridge CA shall not exceed 31 days, and such CAs must meet the requirements specified in section 4.9.12 for issuing Emergency CRLs and are required to notify the DCPA upon Emergency CRL issuance.

4.9.8. Maximum Latency for CRLs

All CRLs for CAs chaining to the Federal Bridge 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

The Issuer CA shall ensure that the certificate status information distributed by it on-line meets or exceeds the requirements for CRL issuance and latency stated in sections 4.9.5, 4.9.7 and 4.9.8. Where offered, OCSP response times shall be no longer than six seconds.

4.9.10. On-line Revocation Checking Requirements

A relying party shall confirm the validity of a Certificate via CRL or OCSP in accordance with section 4.9.6 prior to relying on the Certificate.

4.9.11. Other Forms of Revocation Advertisements Available

An Issuer CA may use other methods to publicize revoked Certificates, provided that:

1. the alternative method is described in its CPS,
2. the alternative method provides authentication and integrity services commensurate with the assurance level of the Certificate being verified, and
3. the alternative method meets the issuance and latency requirements for CRLs stated in sections 4.9.5, 4.9.7, and 4.9.8.

4.9.12. Special Requirements Related to Key Compromise

The Issuer CA or the RA shall use commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects that its Private Key has been compromised. The Issuer CA must have the ability to transition any revocation reason to code to “key compromise”. If a Certificate is revoked because of compromise or suspected compromise, the Issuer CA shall issue a CRL within 18 hours after it receives notice of the compromise or suspected compromise.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request
Not applicable.

4.9.16. Limits on Suspension Period
Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics
Issuer CAs shall make certificate status information available via CRL or OCSP. The Issuer CA shall list revoked Certificates on the appropriate CRL where they remain until one additional CRL is published after the end of the Certificate's validity period, except for EV Code Signing Certificates, which shall remain on the CRL for at least 365 days following the Certificate's validity period.

4.10.2. Service Availability
Issuer CAs shall provide certificate status services 24x7 without interruption.

4.10.3. Optional Features
No stipulation.

4.11. END OF SUBSCRIPTION
The Issuer CA shall allow Subscribers to end their subscription to certificate services by having their Certificate revoked or by allowing the Certificate or applicable Subscriber Agreement to expire without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices
Issuer CAs may not escrow CA Private Keys. Issuer CAs may escrow Subscriber key management keys to provide key recovery services. Issuer CAs shall encrypt and protect escrowed Private Keys with at least the level of security used to generate and deliver the Private Key. For Certificates cross-certified with the FBCA, third parties are not permitted to hold the Subscriber signature keys in trust.

Subscribers and other authorized entities may request recovery of an escrowed Private Key. Entities escrowing Private Keys shall have personnel controls in place that prevent unauthorized access to Private Keys. Key recovery requests can only be made for one of the following reasons:

1. The Subscriber has lost or damaged the private-key token,
2. The Subscriber is not available or is no longer part of the organization that contracted with the Issuer CA for Private Key escrow,
3. The Private Key is part of a required investigation or audit,
4. The requester has authorization from a competent legal authority to access the communication that is encrypted using the key,
5. If key recovery is required by law or governmental regulation, or
6. If the entity contracting with the Issuer CA for escrow of the Private Key indicates that key recovery is mission critical or mission essential.

An entity receiving Private Key escrow services shall:

1. Notify Subscribers that their Private Keys are escrowed,
2. Protect escrowed keys from unauthorized disclosure,
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys,
4. Release escrowed keys only for properly authenticated and authorized requests for recovery, and

5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

Issuer CAs that support session key encapsulation and recovery shall describe their practices in their CPS.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

The Issuer CA shall perform its CA operations from a secure data center equipped with logical and physical controls that make the CA operations inaccessible to non-trusted personnel. The site location and construction, when combined with other physical security protection mechanisms such as guards, door locks, and intrusion sensors, shall provide robust protection against unauthorized access to CA equipment and records. RAs must protect their equipment from unauthorized access in a manner that is appropriate to the level of threat to the RA, including protecting equipment from unauthorized access while the cryptographic module is installed and activated and implementing physical access controls to reduce the risk of equipment tampering, even when the cryptographic module is not installed and activated.

5.1.2. Physical Access

Each Issuer CA and each RA shall protect its equipment (including certificate status servers) from unauthorized access and shall implement physical controls to reduce the risk of equipment tampering. The Issuer CA and all RAs shall store all removable media and paper containing sensitive plain-text information related to CA or RA operations in secure containers. The security mechanisms should be commensurate with the level of threat to the equipment and data.

The Issuer CA shall manually or electronically monitor its systems for unauthorized access at all times, maintain an access log that is inspected periodically, and require two-person physical access to the CA hardware and systems. An Issuer CA shall deactivate and securely store its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module and must not be stored with the cryptographic module or removable hardware associated with remote workstations used to administer the CA equipment or Private Keys.

If the facility housing the CA equipment is ever left unattended, the Issuer CA's administrators shall verify that:

1. the CA is in a state appropriate to the current mode of operation,
2. the security containers are properly secured
3. physical security systems (e.g., door locks, vent covers) are functioning properly, and
4. the area is secured against unauthorized access.

The Issuer CA shall make a person or group of persons explicitly responsible for making security checks. If a group of persons is responsible, the Issuer CA shall maintain a log that identifies who performed the security check. 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 Issuer CA shall maintain a backup power supply and sufficient environmental controls to protect the CA systems and allow the CA to automatically finish pending operations and record the state of equipment before a lack of power or air conditioning causes a shutdown.

5.1.4. Water Exposures
The Issuer CA shall protect its CA equipment from water exposure.

5.1.5. Fire Prevention and Protection
The Issuer CA shall use facilities equipped with fire suppression mechanisms.

5.1.6. Media Storage
Issuer CAs and RAs shall protect all media from accidental damage and unauthorized physical access. Each Issuer CA and each RA shall duplicate and store its audit and archive information in a backup location that is separate from its primary operations facility.

5.1.7. Waste Disposal
Issuer CAs and RAs shall destroy all data (electronic and paper) in accordance with generally accepted procedures for permanently destroying such data.

5.1.8. Off-site Backup
The Issuer CA or RA shall make weekly system backups sufficient to recover from system failure and shall store the backups, including at least one full backup copy, at an offsite location that has procedural and physical controls that are commensurate with its operational location.

5.1.9. Certificate Status Hosting, CMS and External RA Systems
All physical control requirements under this Section 5.1 apply equally to any Certificate Status Hosting, CMS or external RA system.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles
CA and RA personnel acting in trusted roles include CA and RA system administration personnel and personnel involved with identity vetting and the issuance and revocation of Certificates. Issuer CAs and RAs shall distribute the functions and duties performed by persons in trusted roles in a way that prevents one person from circumventing security measures or subverting the security and trustworthiness of the PKI. Senior management of the Issuer CA or the RA shall be responsible for appointing individuals to trusted roles. A list of such personnel shall be maintained and reviewed annually.

The following four trusted roles are defined by this CP, although an Issuer CA or RA may define additional ones:

5.2.1.1. CA Administrators
The CA Administrator is responsible for the installation and configuration of the CA software, including key generation, user and CA accounts, audit parameters, key backup, and key management. The CA Administrator is responsible for performing and securely storing regular system backups of the CA system. Administrators may not issue certificates to Subscribers.

5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel
The Registration Officer role is responsible for issuing and revoking Certificates, including enrollment, identity verification, and compliance with required issuance and revocation steps such as managing the certificate request queue and completing certificate approval checklists as identity vetting tasks are successfully completed.

5.2.1.3. System Administrator/ System Engineer (Operator)
The System Administrator, System Engineer or CA Operator is responsible for installing and configuring CA system hardware, including servers, routers, firewalls, and network configurations.

The System Administrator / Engineer is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditor Role

The Internal Auditor Role is responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if the Issuer CA or RA is operating in accordance with this CP.

5.2.2. Number of Persons Required per Task

Each Issuer CA shall require that at least two people acting in a trusted role (one the CA Administrator and the other not an Internal Auditor) take action requiring a trusted role, such as activating the Issuer CA's Private Keys, generating a CA Key Pair, or creating a backup of a CA Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system, but logical access shall not be achieved using personnel that serve in the Internal Auditor role.

5.2.3. Identification and Authentication for each Role

Issuer CA personnel shall authenticate themselves to the certificate management system before they are allowed access to the systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Individual personnel shall be specifically designated to the four roles defined in Section 5.2.1 above. An individual may assume only one of the Registration Officer, Administrator, or Internal Auditor roles. Individuals designated as Registration Officer or Administrator may also assume the Operator role. An Internal Auditor may not assume any other role.

The Issuer CA and RA may enforce separation of duties using CA equipment, procedurally, or by both means. The CA and RA software and hardware shall identify and authenticate its users and shall ensure that no user identity can assume both an Administrator and a Registration Officer role, assume both the Administrator and Internal Auditor roles, or assume both the Internal Auditor and Registration Officer roles. An individual may not have more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for the operation of the DigiCert PKI and compliance with this CP. Issuer CA and RA personnel and management who purport to act within the scope of this document shall be selected on the basis of loyalty, trustworthiness, and integrity. All trusted roles for Issuer CAs issuing Federated Device Certificates, Client Certificates at Levels 3-US and 4-US (which are intended for interoperability through the Federal Bridge CA at id-fpki-certpcy-mediumAssurance and id-fpki-certpcy-mediumHardware) shall be held by citizens of the United States or the country where the Issuer CA is located. In addition to the above, an individual performing a trusted role for an RA may be a citizen of the country where the RA is located. There is no citizenship requirement for Issuer CA or RA personnel performing trusted roles associated with the issuance of SSL/TLS Server, Code Signing or Client Certificates at Levels 1, 2, 3-CBP, and 4-CBP.

Managerial personnel involved in time-stamping operations must possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures.

The Issuer CA or the RA shall ensure that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CP.

5.3.2. Background Check Procedures

The Issuer CA and RA shall require each person fulfilling a trusted role to undergo identity verification, background checks, and adjudication prior to acting in the role, including verification of the individual's identity, employment history, education, character references, social security number, previous residences, driving records and criminal background. The Issuer CA or RA shall require each individual to appear in-person before a trusted agent whose responsibility it is verify identity. The trusted agent shall verify the identity of the individual using at least one form of government-issued photo identification. Checks of previous residences are over the past three years. All other checks are for the prior five years. The Issuer CA or RA shall verify the highest education degree obtained regardless of the date awarded and shall refresh all background checks at least every ten years. Based upon the information obtained, a competent adjudication authority within the Issuer CA or RA shall adjudicate whether the individual is suitable for the position to which they will be assigned.

5.3.3. Training Requirements

The Issuer CA shall provide skills training to all personnel involved in the Issuer CA's PKI operations. The training must relate to the person's job functions and cover:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by the Issuer CA,
3. authentication and verification policies and procedures,
4. CA/RA security principles and mechanisms,
5. disaster recovery and business continuity procedures,
6. common threats to the validation process, including phishing and other social engineering tactics, and
7. CA/Browser Forum Guidelines.

Issuer CAs shall maintain a record of who received training and what level of training was completed. Issuer CAs and RAs shall ensure that Registration Officers have the minimum skills necessary to satisfactorily perform validation duties before they are granted validation privileges. Where competence was demonstrated in lieu of training, the Issuer CA or RA must maintain supporting documentation.

Issuer CAs and RAs involved with the operation of CMS shall ensure that all personnel who perform duties involving the CMS receive comprehensive training. Issuer CAs and RAs shall create a training (awareness) plan to address any significant change to CMS operations and shall document the execution of the plan.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. The Issuer CA or RA shall make individuals acting in trusted roles aware of any changes to the Issuer CA's or RA's operations. If such operations change, the Issuer CA or RA shall provide documented training, in accordance with an executed training plan, to all trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

Issuer CA or RA employees and agents failing to comply with this CP, whether through negligence or malicious intent, shall be subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management reviews and discusses the incident with the

trusted personnel, management may reassign the employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

Any Issuer CA or RA allowing independent contractors to be assigned to perform trusted roles shall require that they agree to the obligations under this Section 5 (Facility, Management, and Operational Controls) and the sanctions stated above in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

Issuer CAs and RAs shall provide personnel in trusted roles with the documentation necessary to perform their duties.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

Issuer CA and RA systems (including any CMS) shall require identification and authentication at system logon. Important system actions shall be logged to establish the accountability of the operators who initiate such actions.

Issuer CAs and RAs shall enable all essential event auditing capabilities of its CA or RA applications in order to record all events related to the security of the CA or RA, including those listed below. A message from any source received by the Issuer CA requesting an action related to the operational state of the CA is an auditable event. If the Issuer CA's applications cannot automatically record an event, the Issuer CA shall implement manual procedures to satisfy the requirements. For each event, the Issuer CA shall record the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. The Issuer CA shall make all event records available to its auditors as proof of the Issuer CA's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to certificate subject Private Keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
SECRET KEY STORAGE

Auditable Event
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Certificate issuance
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs and OCSP entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
Installation of a Hardware Security Modules
Removal of HSMs
Destruction of HSMs
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Backup of the internal CA database
Restoration from backup of the internal CA database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
Loading HSMs with Certificates
Shipment of HSMs
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System

Auditable Event
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA components
Access to a CA component
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CP or CPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

The Issuer CA or RA shall, at least every two months, review system logs, make system and file integrity checks, and make a vulnerability assessment. The Issuer CA or RA may use automated tools to scan for anomalies or specific conditions. During its review, the Issuer CA or RA shall verify that the logs have not been tampered with, examine any statistically significant set of security audit data generated since the last review, and make a reasonable search for any evidence of malicious activity. The Issuer CA or RA shall briefly inspect all log entries and investigate any detected anomalies or irregularities. The Issuer CA or RA shall make a summary of the review available to its auditors upon request. The Issuer CA of RA shall document any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

The Issuer CA and RA shall retain audit logs on-site until after they are reviewed. The individual who removes audit logs from the Issuer CA's or RA's systems must be different than the individuals who control the Issuer CA's signature keys.

5.4.4. Protection of Audit Log

The Issuer CA and RA shall implement procedures that protect archived data from destruction prior to the end of the audit log retention period. The Issuer CA and RA shall configure its systems and establish operational procedures to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. The Issuer CA's off-site storage location must be a safe and secure location that is separate from the location where the data was generated.

The Issuer CA and RA shall make records available if required for the purpose of providing evidence of the correct operation of time-stamping services for the purpose of legal proceedings. The Issuer CA shall make its audit logs available to auditors upon request.

5.4.5. Audit Log Backup Procedures

On at least a monthly basis, the Issuer CA and RA shall make backups of audit logs and audit log summaries and send a copy of the audit log off-site.

5.4.6. Audit Collection System (internal vs. external)

The Issuer CA or RA may use automatic audit processes, provided that they are invoked at system startup and end only at system shutdown. If an automated audit system fails and the integrity of the system or confidentiality of the information protected by the system is at risk, the DCPA shall be notified and determine whether to suspend the Issuer CA's or RA's operations until the problem is remedied.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

The Issuer CA shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate issuance process. The Issuer CA shall also routinely assess the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Issuer CA has in place to control such risks. The Issuer CA's auditors should review the security audit data checks for continuity and alert the appropriate personnel of any events, such as repeated failed actions, requests for privileged information, attempted access of system files, and unauthenticated responses.

5.5. RECORDS ARCHIVAL

The Issuer CA shall comply with any record retention policies that apply by law. The Issuer CA shall include sufficient detail in archived records to show that a Certificate was issued in accordance with the CPS.

5.5.1. Types of Records Archived

The Issuer CA shall retain the following information in its archives (as such information pertains to the Issuer CA's CA operations):

1. Any accreditation of the Issuer CA,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA,
4. System and equipment configurations, modifications, and updates,
5. Certificate and revocation requests,
6. Identity authentication data,
7. Any documentation related to the receipt or acceptance of a Certificate or token,
8. Subscriber Agreements,
9. Issued certificates,
10. A record of certificate re-keys,
11. CRLs for CAs cross-certified with the Federal Bridge CA,
12. Any data or applications necessary to verify an archive's contents,
13. Compliance auditor reports,
14. Any changes to the Issuer CA's audit parameters,
15. Any attempt to delete or modify audit logs,
16. Key generation,
17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a revocation request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP or CPS.

5.5.2. Retention Period for Archive

The Issuer CA shall retain archived data associated with Level 3, Level 4, and federated device Certificates for 10.5 years. For all other Certificates, the Issuer CA shall retain archived data for at least 7.5 years. RAs supporting Certificates that are not cross-certified with the FBCA may retain archived data for a shorter period of time if the practice is documented in a RPS or document retention policy.

5.5.3. Protection of Archive

The Issuer CA shall store its archived records at a secure off-site location in a manner that prevents unauthorized modification, substitution, or destruction. No unauthorized user may access, write, or delete the archives. If the original media cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media. The Issuer CA shall maintain any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

5.5.4. Archive Backup Procedures

If an Issuer CA or RA chooses to back up its archive records, then the Issuer CA or RA shall describe how its records are backed up and managed in its CPS or a referenced document.

5.5.5. Requirements for Time-stamping of Records

The Issuer CA shall automatically time-stamp archive records as they are created. Cryptographic time-stamping of archive records is not required; however, the Issuer CA shall synchronize its system time at least every eight hours using a real time value traceable to a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6. Archive Collection System (internal or external)

The Issuer CA shall collect archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

The Issuer CA may archive data manually or automatically. If automatic archival is implemented, the Issuer CA shall synchronize its archived data on a daily basis.

The Issuer CA may allow Subscribers to obtain a copy of their archived information. Otherwise, the Issuer CA shall restrict access to archive data to authorized personnel in accordance with the Issuer CA's internal security policy and shall not release any archived information except as allowed by law. CAs shall state in their CPS the details of how they create, verify, package, transmit, and store archived information.

5.6. KEY CHANGEOVER

The Issuer CA shall periodically change its Private Keys in a manner set forth in the CPS that prevents downtime in the Issuer CA's operation. After key changeover, the Issuer CA shall sign Certificates using only the new key. The Issuer CA shall still protect its old Private Keys and shall make the old Certificate available to verify signatures until all of the Certificates signed with the Private Key have expired.

Issuer CAs cross-certified with the FBCA must be able to continue to interoperate with the FBCA after the FBCA performs a key rollover, whether or not the FBCA DN is changed. Issuer CAs either must establish key rollover Certificates as described above or must obtain a new CA Certificate for the new Public Key from the issuers of their current Certificates.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

The Issuer CA shall develop and implement procedures to be followed in the event of a serious security incident or system compromise. Required documentation includes, but is not limited to, an Incident Response Plan, a Disaster Recovery or Business Continuity Plan (DR/BCP), and related resources. The Issuer CA shall review, test, and update its Incident Response Plan and DR/BCP, and supporting procedures, at least annually.

The Issuer CA shall require that any CMS have documented incident handling procedures that are approved by the head of the organization responsible for operating the CMS. If the CMS is compromised, the Issuer CA shall revoke all Certificates issued to the CMS, if applicable. The Issuer CA and its RAs shall also assess any damage caused by the CMS compromise, revoke all potentially compromised Subscriber Certificates, notify affected subscribers of the revocation, and re-establish the operation of the CMS.

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

The Issuer CA shall make regular back-up copies of its Private Keys and store them in a secure off-site location. The Issuer CA shall also make regular system back-ups on at least a weekly basis. If a disaster causes the Issuer CA's operations to become inoperative, the Issuer CA shall, after ensuring the integrity of the CA systems, re-initiate its operations on replacement hardware using backup copies of its software, data, and Private Keys at a secure facility. The Issuer CA shall give priority to reestablishing the generation of certificate status information. If the Private Keys are destroyed, the Issuer CA shall reestablish operations as quickly as possible, giving priority to generating new Key Pairs.

5.7.3. Entity Private Key Compromise Procedures

If the Issuer CA suspects that a CA Private Key is comprised or lost then the Issuer CA shall follow its Incident Response Plan and immediately assess the situation, determine the degree and scope of the incident, and take appropriate action. Issuer CA personnel shall report the results of the investigation. The report must detail the cause of the compromise or loss and the measures should be taken to prevent a reoccurrence. If there is a compromise or loss, the Issuer CA shall notify any affiliated entities so that they may issue CRLs revoking cross-Certificates issued to the Issuer CA and shall notify interested parties and make information available that can be used to identify which Certificates and time-stamp tokens affected, unless doing so would breach the privacy of the Issuer CA's user or the security of the Issuer CA's services.

Following revocation of a CA Certificate and implementation of the Issuer CA's Incident Response Plan, the Issuer CA shall generate a new CA Key Pair and sign a new CA Certificate in accordance with its CPS. The Issuer CA shall distribute the new self-signed Certificate in accordance with Section 6.1.4. The Issuer CA shall cease its CA operations until appropriate steps are taken to recover from the compromise and restore security.

5.7.4. Business Continuity Capabilities after a Disaster

Stated goals of the Issuer CA's DR/BCP shall include that certificate status services be minimally affected by any disaster involving the Issuer CA's primary facility and that other services resume as quickly as possible following a disaster. The Issuer CA shall establish a secure facility in at least one secondary, geographically diverse location to ensure that its directory and on-line status servers, if any, remain operational in the event of a physical disaster at the Issuer CA's main site. The Issuer CA shall provide notice at the earliest feasible time to all interested parties if a disaster physically damages the Issuer CA's equipment or destroys all copies of the Issuer CA's signature keys.

5.8. CA OR RA TERMINATION

If an Issuer CA's operations are terminated, the Issuer CA shall provide notice to interested parties and shall transfer its responsibilities and records to successor entities. The Issuer CA may allow a successor to re-issue Certificates if the successor has all relevant permissions to do so and has operations that are at least as secure the Issuer CA's. If a qualified successor does not exist, the Issuer CA shall transfer all relevant records to a government supervisory or legal body.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

All keys must be generated using a FIPS-approved method or equivalent international standard.

Issuer CAs shall generate cryptographic keying material on a FIPS 140 level 3 validated cryptographic module using multiple individuals acting in trusted roles. When generating key material, the Issuer CA shall create auditable evidence to show that the Issuer CA enforced role separation and followed its key generation process.

An independent third party shall validate that each CA key, including any root or intermediate CA keys associated with a Certificate cross-certified with the FBCA and each Root CA Key (for Certificates not cross-certified with the FBCA), is generated in accordance with this CP either by having the independent third party witness the key generation or by examining a signed and documented record of the key generation.

Subscribers who generate their own keys shall use a FIPS-approved method and either a validated hardware or validated software cryptographic module, depending on the level of assurance desired. Keys for Level 3 Hardware or Level 4 Biometric Certificates must be generated on validated hardware cryptographic modules using a FIPS-approved method. Subscribers who generate their own keys for a Qualified Certificate on an SSCD shall ensure that the SSCD meets the requirements of CWA 14169 and that the Public Key to be certified is from the Key Pair generated by the SSCD.

6.1.2. Private Key Delivery to Subscriber

If the Issuer CA, a CMS, or an RA generates keys on behalf of the Subscriber, then the entity generating the key shall deliver the Private Key securely (encrypted) to the Subscriber. The entity may deliver Private Keys to Subscribers electronically or on a hardware cryptographic module / SSCD. In all cases:

1. Except where escrow/backup services are provided, the key generator may not retain a copy of the Subscriber's Private Key after delivery,
2. The key generator shall protect the Private Key from activation, compromise, or modification during the delivery process,
3. The Subscriber shall acknowledge receipt of the Private Key(s), and
4. The key generator shall deliver the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, the key generator maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
    b. For electronic delivery of Private Keys, the key generator encrypting key material using a cryptographic algorithm and key size at least as strong as the Private Key. The key generator shall deliver activation data using a separate secure channel.

The entity assisting with Subscriber key generation shall maintain a record of the Subscriber's acknowledgement of receipt of the device containing the Subscriber's Key Pair. A CMS or RA providing key delivery services shall provide a copy of this record to the Issuer CA.

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers shall deliver their Public Keys to the Issuer CA in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key. The certificate request process shall ensure that the Applicant possesses the Private Key associated with the Public Key presented for certification. If cryptography is used to achieve the binding, the cryptography 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

The Issuer CA shall provide its Public Keys to Relying Parties in a secure fashion and in a manner that precludes substitution attacks. The Issuer CA may deliver its CA Public Keys to Relying Parties as (i) specified in a certificate validation or path discovery policy file, (ii) trust anchors in commercial browsers and operating system root stores, and/or (iii) roots signed by other CAs. The Issuer CA may distribute Public Keys that are part of an updated signature Key Pair as a self-signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. All accreditation authorities supporting DigiCert Certificates and all application software providers are permitted to redistribute any Root Certificate that is issued under this CP.

6.1.5. Key Sizes

For signing Certificates issued with policy OIDs of 2.16.840.1.114412.1.11, 2.16.840.1.114412.1.12, or within the policy OID arc of 2.16.840.1.114412.4 and for signing CRLs and certificate status server responses for such Certificates, the Issuer CA shall use at least a 2048-bit RSA Key or 384-bit ECDSA Key with SHA-256 (or a hash algorithm that is equally or more resistant to a collision attack). Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

The Issuer CA shall only issue end-entity Certificates that contain at least 2048-bit Public Keys for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms. The Issuer CA may require higher bit keys in its sole discretion.

Any Certificates (whether CA or end-entity) expiring after 12/31/2030 must be at least 3072 bit for RSA and 256 bit for ECDSA.

The Issuer CA and Subscribers may fulfill the transmission security requirements of this CP using TLS or another protocol that provides similar security, provided the protocol requires at least AES 128 bits or equivalent for the symmetric key and at least 2048-bit RSA or equivalent for the asymmetric keys (and at least 3072-bit RSA or equivalent for asymmetric keys after 12/31/2030).

6.1.6. Public Key Parameters Generation and Quality Checking

The Issuer CA shall generate Public Key parameters for signature algorithms and perform parameter quality checking in accordance with FIPS 186.

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

The Issuer CA shall include key usage extension fields that specify the intended use of the Certificate and technically limit the Certificate's functionality in X.509v3-compliant software.

The use of a specific key is determined by the key usage extension in the X.509 Certificate.

CA Certificates shall have two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the Certificate shall also set the digitalSignature bit.

The Issuer CA shall not issue Level 4 Certificates that are certified for both signing and encryption. The use of a single key for encryption and signature is discouraged, and Issuer CAs should issue Subscribers two Key Pairs—one for key management and one for digital signature and authentication. However, for support of legacy applications, other Certificates, including those at Levels 1, 2 and 3, may include a single key for use with encryption and signature. Such dual-use Certificates must:

1. be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in this CP,
2. never assert the non-repudiation key usage bit, and
3. not be used for authenticating data that will be verified on the basis of the dual-use Certificate at a future time.

Subscriber Certificates assert key usages based on the intended application of the Key Pair. In particular, Certificates to be used for digital signatures (including authentication) set the digitalSignature and/or nonRepudiation bits. Certificates to be used for key or data encryption shall set the keyEncipherment and/or dataEncipherment bits. Certificates to be used for key agreement shall set the keyAgreement bit.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

The Issuer CA and all systems that sign OCSP responses or CRLs in order to provide certificate status services shall use cryptographic hardware modules validated to FIPS 140-2 Level 3 and International Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) 14169 EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in the European Union (EU).

Cryptographic module requirements for subscribers and registration authorities are shown in the table below.

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Adobe Signing Certificates	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 3 (Hardware)
Level 1 - Rudimentary	N/A	FIPS 140 Level 1 (Hardware or Software)
Level 2 – Basic	FIPS 140 Level 1 (Hardware or Software)	FIPS 140 Level 1 (Hardware or Software)
Level 3 - Medium	FIPS 140 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Level 4, Medium Hardware, Biometric,	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
EU QC on SSCD	EAL 4 Augmented (Hardware)	EAL 4 Augmented (Hardware)

For EV Code Signing Certificates, the Issuer CA shall ensure that the Private Key is properly generated, stored, and used in a cryptomodule that meets or exceeds the requirements of FIPS 140 level 2.

6.2.1.1. Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. Effective January 1, 2017, all cryptographic modules for Custodial Subscriber Key Stores for certificates issued at Levels 2, 3-US, 3-CBP, 4-US, and 4-CBP shall be no less than FIPS 140 Level 2 Hardware and authentication to activate the private key associated with a given certificate shall require authentication commensurate with the assurance level of the certificate.

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

The Issuer CA shall ensure that multiple trusted personnel are required to act in order to access and use an Issuer CA's Private Keys, including any Private Key backups.

6.2.3. Private Key Escrow

The Issuer CA shall not escrow its signature keys. Subscribers may not escrow their private signature keys. The Issuer CA may escrow Subscriber Private Keys used for encryption in order to provide key recovery as described in section 4.12.1.

6.2.4. Private Key Backup

The Issuer CA shall backup its CA, CRL, and certificate status Private Keys under multi-person control and shall store at least one backup off site. The Issuer CA shall protect all copies of its CA, CRL, and certificate status Private Keys in the same manner as the originals.

The Issuer CA may provide backup services for Private Keys that are not required to be maintained in cryptographic hardware. Access to Private Key backups shall be secured in a manner that only the Subscriber can control the Private Key. The Issuer CA may not backup Level 4 subscriber private signature keys. The Issuer CA may not store backup keys in a plain text form outside of the cryptographic module. Storage that contains backup keys shall provide security controls that are consistent with the protection provided by the Subscriber's cryptographic module.

6.2.5. Private Key Archival

The Issuer CA shall not archive its Private Keys and shall not allow the archival of any Private Keys associated with EU Qualified Certificates.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. The Issuer CA and RA shall never allow their Private Keys to exist in plain text outside of the cryptographic module. The Issuer CA shall only export its Private Keys from the cryptographic module to perform CA key backup procedures. When transported between cryptographic modules, the Issuer CA shall encrypt the Private Key and protect the keys used for encryption from disclosure.

6.2.7. Private Key Storage on Cryptographic Module

The Issuer CA shall store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140 Level 3 and EAL 4+.

6.2.8. Method of Activating Private Key

The Issuer CA shall activate its Private Keys in accordance with the specifications of the cryptographic module manufacturer. Subscribers are solely responsible for protecting their Private

Keys. At a minimum, Subscribers must authenticate themselves to the cryptographic module before activating their Private Keys. Entry of activation data shall be protected from disclosure.

6.2.9. Method of Deactivating Private Key

The Issuer CA shall deactivate its Private Keys and store its cryptographic modules in secure containers when not in use. The Issuer CA shall prevent unauthorized access to any activated cryptographic modules.

6.2.10. Method of Destroying Private Key

The Issuer CA shall use individuals in trusted roles to destroy CA, RA, and status server Private Keys when they are no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed. For software cryptographic modules, the Issuer CA may destroy the Private Keys by overwriting the data. For hardware cryptographic modules, the Issuer CA may destroy the Private Keys by executing a "zeroize" command. Physical destruction of hardware is not required.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

The Issuer CA shall archive a copy of each Public Key.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

All Certificates, including renewed Certificates, have maximum validity periods of:

Type	**Private Key Use**	**Certificate Term**
Root CA	20 years	25 years
Sub CA	12 years	15 years
FBCA-Cross-certified Sub CAs	6 years (period of key use for signing certificates)	10 years (key still signs CRLs, OCSP responses, and OCSP responder certificates)
IGTF Cross-certified Sub CA*	6 years	15 years
CRL and OCSP responder signing	3 years	31 days†
OV SSL/TLS	No stipulation	as specified in section 6.3.2 of the Baseline Requirements
EV SSL/TLS	No stipulation	825 days
Code Signing Certificate issued to Subscriber under the Minimum Requirements for Code Signing Certificates or the EV Code Signing Guidelines	No stipulation	39 months
EV Code Signing Certificate issued to Signing Authority	No stipulation	123 months
Time Stamping Authority	15 months	135 months
Object Signing Certificate and Document Signing	No stipulation‡	123 months
FBCA and IGTF Client used for signatures (including EU Qualified Certificates)	36 months	36 months
FBCA and IGTF Client used for key management	36 months	36 months
Client for all other purposes (FBCA or IGTF	36 months	36 months

compliant)		
Client for all other purposes (non FBCA and IGTF certs)	No stipulation	60 months
IGTF on hardware	60 months	13 months

* IGTF signing Certificates must have a lifetime that is at least twice the maximum lifetime of an end entity Certificate.
† OCSP responder and CRL signing Certificates associated with a PIV-I Certificate may only have a maximum certificate validity period of 31 days.
‡ Code and content signers cross-certified with FBCA may use their Private Keys for three years; the lifetime of the associated Public Keys shall not exceed eight years.

Relying parties may still validate signatures generated with these keys after expiration of the Certificate.

Private keys associated with self-signed root Certificates that are distributed as trust anchors are used for a maximum of 20 years.

The Issuer CA may retire its CA Private Keys before the periods listed above to accommodate key changeover processes. The Issuer CA shall not issue a Subscriber Certificate with an expiration date that is past the Issuer CA's public key expiration date or that exceeds the routine re-key identification requirements specified in Section 3.1.1.

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

The Issuer CA shall generate activation data that has sufficient strength to protect its Private Keys. If the Issuer CA uses passwords as activation data for a signing key, the Issuer CA shall change the activation data upon rekey of the CA Certificate. The Issuer CA may only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

6.4.2. Activation Data Protection

The Issuer CA shall protect data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Activation data shall be:

- memorized
- biometric in nature, or
- recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The Issuer CA shall require personnel to memorize and not write down their password or share their passwords with other individuals. The Issuer CA shall implement processes to temporarily lock access to secure CA processes if a certain number of failed log-in attempts occur as set forth in the applicable CPS.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

The Issuer CA shall configure its systems, including any remote workstations, to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

The Issuer CA shall authenticate and protect all communications between a trusted role and its CA system.

All Certificate Status Servers interoperating with cross-certified environments must:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges to limit users to their assigned roles,
3. enforce domain integrity boundaries for security critical processes, and
4. support recovery from key or system failure.

A CMS must have the following computer security functions:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage privileges of users to limit users to their assigned roles,
3. generate and archive audit records for all transactions, (see Section 5.4)
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

In operating its CA, the Issuer CA shall use only:

1. Commercial off-the-shelf software that was designed and developed under a formal and documented development methodology,
2. Hardware and software developed specifically for the Issuer CA by verified personnel, using a structured development approach and a controlled development environment,
3. Open source software that meets security requirements through software verification & validation and structured development/life-cycle management,
4. Hardware and software purchased and shipped in a fashion that reduces the likelihood of tampering, and
5. For CA operations, hardware and software that is dedicated only to performing the CA functions.

The Issuer CA shall take proper care to prevent malicious software from being loaded onto the CA equipment. The Issuer CA shall scan all hardware and software for malicious code on first use and periodically thereafter. The Issuer CA shall purchase or develop updates in the same manner as original equipment, and shall use trusted trained personnel to install the software and equipment. The Issuer CA shall not install any software on its CA systems that are not part of the CA's operations.

The Issuer CA shall use a formal configuration management methodology for installation and ongoing maintenance of any CMS. Any modifications and upgrades to a CMS shall be documented and controlled. The Issuer CA shall implement a mechanism for detecting unauthorized modification to a CMS.

6.6.2. Security Management Controls

The Issuer CA shall establish formal mechanisms to document, control, monitor, and maintain the installation and configuration of its CA systems, including any modifications or upgrades. The Issuer CA's change control processes shall include procedures to detect unauthorized modification to the Issuer CA's systems and data entries that are processed, logged and tracked for any security-related changes to CA systems, firewalls, routers, software and other access controls. When loading software onto a CA system, the Issuer CA shall verify that the software is the correct version and is supplied by the vendor free of any modifications. The Issuer CA shall verify the integrity of software used with its CA processes at least once a week.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

The Issuer CA shall document and control the configurations of its systems, including any upgrades or modifications made. The Issuer CA shall implement a process for detecting unauthorized modifications to its hardware or software and for installing and maintaining its systems.

The Issuer CA and its RAs shall implement appropriate network security controls, including turning off any unused network ports and services and only using network software that is necessary for the proper functioning of the CA systems. The Issuer CA shall implement the same network security controls to protect a CMS as used to protect its other CA equipment.

6.8. TIME-STAMPING

Issuer CAs shall ensure that the accuracy of clocks used for time-stamping are 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

7.1.1. Version Number(s)

Issuer CAs shall issue X.509 version 3 Certificates.

7.1.2. Certificate Extensions

Issuer CAs shall use certificate extensions in accordance with applicable industry standards, including RFC 3280/5280. Issuer CAs shall not issue Certificates with a critical private extension. IGTF Certificates must comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

7.1.3. Algorithm Object Identifiers

Issuer CAs shall sign Certificates using one of the following algorithms:

id-dsa-with-sha1	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 3}
sha-1WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 5}
sha256WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 11}
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi (113549) pkcs(1) pkcs-1(1) 10 }
ecdsa-with-SHA1	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) 1 }
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

If an Issuer CA signs Certificates using RSA with PSS padding, the Issuer CA may use an RSA signature with PSS padding with the following algorithms and OIDs:

id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }

Issuer CAs and Subscribers may generate Key Pairs using the following:

id-dsa	{iso(1) member-body(2) us(840) x9-57(10040) x9cm(4) 1}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}
Dhpublicnumber	{iso(1) member-body(2) us(840) ansi-x942(10046) number-type(2) 1}
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }
id-keyExchangeAlgorithm	[joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) infosec(1) algorithms(1) 22]

If an Issuer CA issues a non-CA Certificate for a federal agency and the Certificate contains an elliptic curve Public Key, the Issuer CA shall specify one of the following named curves:

ansip192r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 1 }
ansit163k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 1 }
ansit163r2	{ iso(1) identified-organization(3) certicom(132) curve(0) 15 }
ansip224r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 33 }
ansit233k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 26 }
ansit233r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 27 }
ansip256r1	{ iso(1) member-body(2) us(840) 10045 curves(3) prime(1) 7 }
ansit283k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 16 }
ansit283r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 17 }
ansip384r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 34 }
ansit409k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 36 }
ansit409r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 37 }
ansip521r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 35 }
ansit571k1	{ iso(1) identified-organization(3) certicom(132) curve(0) 38 }
ansit571r1	{ iso(1) identified-organization(3) certicom(132) curve(0) 39 }

7.1.4. Name Forms

Issuer CAs shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 3280/5280. Issuer CAs shall include a unique serial number in each Certificate. The Issuer CA shall restrict OU fields from containing Subscriber information that is not verified in accordance with Section 3.

7.1.5. Name Constraints

Issuer CAs may include name constraints in the nameConstraints field when appropriate.

7.1.6. Certificate Policy Object Identifier

When an Issuer CA issues a Certificate containing one of the policy identifiers set forth in Section 1.2, it asserts that the Certificate is managed in accordance with the policy that is identified herein.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics
Issuer CAs may include brief statements in the Policy Qualifier field of the Certificate Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension
No stipulation.

7.2. CRL PROFILE

7.2.1. Version number(s)
Issuer CAs shall issue version 2 CRLs that conform to RFC 3280/5280.

7.2.2. CRL and CRL Entry Extensions
Issuer CAs shall use CRL extensions that conform with the Federal PKI X.509 CRL Extensions Profile.

7.3. OCSP PROFILE
Issuer CAs shall operate an OCSP service in accordance with RFC 2560.

7.3.1. Version Number(s)
Issuer CAs shall support version 1 OCSP requests and responses.

7.3.2. OCSP Extensions
No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS
The policies in this CP are designed to meet or exceed the requirements of generally accepted and developing industry standards, including the WebTrust Program for Certification Authorities. For Issuer CAs chained to the FBCA, the auditor letter of compliance shall meet FPKIPA Audit Requirements. All Issuer CAs shall ensure that audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT
On at least an annual basis, Issuer CAs shall retain an independent auditor who shall assess the Issuer CA's compliance with this CP and its CPS. This audit must cover CMSs, Sub CAs, RAs, and each status server that is specified in a certificate issued by the Issuer CA. Any independent entity interoperating within the DigiCert PKI shall submit its practices statement and the results of its compliance audit to the DCMA on an annual basis for review and approval.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

8.3. THE ISSUER CA SHALL USE AN AUDITOR THAT MEETS SECTION 8.2 OF THE BASELINE REQUIREMENTS (FOR WEBTRUST) AND SECTION 8.2 OF THE FEDERAL BRIDGE CP (FOR CERTIFICATES CROSS-CERTIFIED UNDER THE FEDERAL BRIDGE CA). ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY
The Issuer CA shall utilize independent auditors that do not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the Issuer CA.

8.4. TOPICS COVERED BY ASSESSMENT
The audit must conform to industry standards, cover the Issuer CA's compliance with its business practices disclosure, and evaluate the integrity of the Issuer CA's PKI operations. The audit must verify that each Issuer CA is compliant with this CP and any MOA between it and any other PKI.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CP, the CPS, or any other contractual obligations related to the Issuer CA's services, then (1) the auditor shall document the discrepancy, (2) the auditor shall promptly notify the Issuer CA and the DCPA, and (3) the Issuer CA and the DCPA shall develop a plan to cure the noncompliance. The DCPA shall also notify any affected cross-certifying entity and any relevant government accrediting body. The Issuer CA shall submit the plan to the DCPA for approval and to any third party that the Issuer CA is legally obligated to satisfy. The DCPA may require additional action if necessary to rectify any significant issues created by the non-compliance, including requiring revocation of affected Certificates.

8.6. COMMUNICATION OF RESULTS

The results of each audit shall be reported to the DCPA for review and approval. The results shall also be communicated to any third party entities entitled by law, regulation, or agreement to receive a copy of the audit results. On an annual basis, the DCPA shall submit an audit compliance package to the Federal PKI Policy Authority prepared in accordance with the "Compliance Audit Requirements" document, which shall include an assertion that all PKI components have been audited, including any components that may be separately managed and operated. The package shall identify the versions of the CP and CPS used in the assessment.

8.7. SELF-AUDITS

The Issuer CA shall perform regular internal audits of its operations, personnel, and compliance with this CP using a randomly selected sample of Certificates issued since the last internal audit. The Issuer CA shall self-audit at least three percent of SSL/TLS Certificates and EV Code Signing Certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

Issuer CAs may charge fees for certificate issuance and renewal.

9.1.2. Certificate Access Fees

Issuer CAs may charge fees for access to their databases of Certificates.

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

Issuer CAs shall maintain Errors and Omissions / Professional Liability Insurance of at least $1 million per occurrence from an insurance company rated no less than A- as to Policy Holder's Rating in the current edition of Best's Insurance Guide (or with an association of companies, each of the members of which are so rated).

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities
No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information
Issuer CAs shall specify what constitutes confidential information in its CPS.

9.3.2. Information Not Within the Scope of Confidential Information
Issuer CAs may treat any information not listed as confidential in the CPS as public information.

9.3.3. Responsibility to Protect Confidential Information
Issuer CAs shall contractually obligate employees, agents, and contractors to protect confidential information. Issuer CAs shall provide training to employees on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan
Issuer CAs shall create and follow a publicly posted privacy policy that specifies how the Issuer CA handles personal information.

9.4.2. Information Treated as Private
Issuer CAs shall treat all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. The Issuer CA shall protect private information in its possession using a reasonable degree of care and appropriate safeguards. The Issuer CA shall not distribute Certificates that contain the UUID in the subject alternative name extension via publicly accessible repositories (e.g., LDAP, HTTP).

9.4.3. Information Not Deemed Private
Private information does not include Certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information
Issuer CAs are responsible for securely storing and protecting private information.

9.4.5. Notice and Consent to Use Private Information
Subscribers must consent to the global transfer and publication of any personal data contained in Certificates.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process
Issuer CAs may disclose private information, without notice, when required to do so by law or regulation.

9.4.7. Other Information Disclosure Circumstances
No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS
Issuer CAs shall not knowingly violate the intellectual property rights of any third party.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties
Issuer CAs must represent to DigiCert, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP, their CPS, and all applicable laws and regulations.

9.6.2. RA Representations and Warranties

At a minimum, Issuer CAs shall require RAs operating on their behalf to represent that they have followed this CP and the relevant CPS when participating in the issuance and management of Certificates.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, each Subscriber shall represent to DigiCert and the Issuer CA that the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information and communication to the Issuer CA and RA,
3. Confirm the accuracy of Certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify the Issuer CA if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Use the Certificate only for authorized and legal purposes, consistent with the relevant CPS and Subscriber Agreement, including only installing SSL/TLS Server Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and
6. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

9.6.4. Relying Party Representations and Warranties

Relying Parties must follow the procedures and make the representations required by the relevant CPS and in the applicable Relying Party Agreement prior to relying on or using a Certificate.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

Except as expressly stated otherwise herein or as limited by law, DigiCert disclaims all warranties and obligations related to this CP. A fiduciary duty is not created simply because an entity uses services offered within the DigiCert PKI.

9.8. LIMITATIONS OF LIABILITY

Issuer CAs may limit their liability to any extent not otherwise prohibited by this CP, provided that the Issuer CA remains responsible for complying with this CP and the Issuer CA's CPS.

9.9. INDEMNITIES

9.9.1. Indemnification by an Issuer CA

Issuer CAs are required to indemnify DigiCert for any violation of this CP.

9.9.2. Indemnification by Subscribers

Issuer CAs shall include any indemnification requirements for Subscribers in their CPS and in their Subscriber Agreements.

9.9.3. Indemnification by Relying Parties

Issuer CAs shall include any indemnification requirements for Relying Parties in their CPS.

9.10. TERM AND TERMINATION

9.10.1. Term

This CP and any amendments are effective when published to DigiCert's online repository and remain in effect until replaced with a newer version.

9.10.2. Termination

This CP and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

DigiCert will communicate the conditions and effect of this CP's termination via the DigiCert Repository. The communication will specify which provisions survive termination. At a minimum, responsibilities related to protecting confidential information will survive termination.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert accepts digitally signed or paper notices related to this CP that are addressed to the locations specified in Section 2.2 of this CP. Notices are deemed effective after the sender receives a valid and digitally signed acknowledgment of receipt from DigiCert. If an acknowledgement of receipt is not received within five days, the sender must resend the notice in paper form to the street address specified in Section 2.2 using either a courier service that confirms delivery or via certified or registered mail with postage prepaid and return receipt requested.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

The DCPA determines what amendments should be made to this CP. Amendments are made by posting an updated version of the CP to the online repository. Controls are in place to reasonably ensure that this CP is not amended and published without the prior authorization of the DCPA. The DCPA reviews this CP annually.

9.12.2. Notification Mechanism and Period

DigiCert will post notice on its website of any proposed significant revisions to this CP. Although DigiCert may include a final date for receipt of comments and the proposed effective date, DigiCert is not required to have a fixed notice-and-comment period.

9.12.3. Circumstances under which OID Must Be Changed

If the DCPA determines an amendment necessitates a change in an OID, then the revised version of this CP will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

Before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution, a party must notify DigiCert of the dispute with a view to seek dispute resolution.

9.14. GOVERNING LAW

For disputes involving Qualified Certificates, the national law of the relevant Member State shall govern. For all other certificates, the laws of the state of Utah shall govern the interpretation, construction, and enforcement of this CP and all proceedings related hereunder, including tort claims, without regard to any conflicts of law principles, and Utah shall be the non-exclusive venue and shall have jurisdiction over such proceedings.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CP is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5's Notice and Consent to Use

Private Information contained in Certificates, each Issuer CA shall meet the requirements of European data protection laws and shall establish and maintain appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

Issuer CAs shall contractually obligate each RA involved in Certificate issuance to comply with this CP and applicable industry guidelines. Issuer CAs shall contractually obligate parties using products and services issued under this CP, such as Subscribers and Relying Parties, to the relevant provisions herein. This CP does not give any third party rights under such agreements.

9.16.2. Assignment

Entities operating under this CP may not assign their rights or obligations without the prior written consent of DigiCert.

9.16.3. Severability

If a provision of this CP is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP will remain valid and enforceable.

9.16.4. Enforcement (attorneys' fees and waiver of rights)

DigiCert may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. DigiCert's failure to enforce a provision of this CP does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this CP. To be effective, waivers must be in writing and signed by DigiCert.

9.16.5. Force Majeure

DigiCert is not liable for a delay or failure to perform an obligation under this CP to the extent that the delay or failure is caused by an occurrence beyond DigiCert's reasonable control. The operation of the Internet is beyond DigiCert's reasonable control.

9.17. OTHER PROVISIONS

No stipulation.