DigiCert

Certificate Policy

DigiCert, Inc.
Version 4.01
August 26, 2010

Suite 200
Canopy Building II
355 South 520 West
Lindon, UT 84042
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. 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 CP defines fourteen Object Identifiers (OIDs) that represent various uses and levels of trust for digitally signed objects: two for SSL certificates, five for client certificates, three for Personal Identify Verification cards, one for code signing certificates, two for EU qualified certificates, and one for time-stamping. This document also specifies the policies DigiCert uses to meet the current requirements of the "Guidelines for the Issuance and Management of Extended Validation Certificates," published by the Certification Authority / Browser Forum ("CAB Forum"). DigiCert always conforms to the current version of the CAB Forum Guidelines published at http://www.cabforum.org (the "EV Guidelines"). If any inconsistency exists between this CP and the EV Guidelines, the EV Guidelines 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 Federal Bridge CP, the Citizen and Commerce Class Common CP, NIST 800-63, the Kantara Initiative and the European Directive 1999/93/EC.

Personal Identity Verification – Interoperable (PIV-I) cards issued under this CP are intended to technically interoperate with Federal PIV Card readers and applications. Reliance on PIV-I Cards requires compliance with technical specifications and specific trust elements. PIV policies for PIV-I Hardware, PIV-I Card Authentication, and PIV-I Content Signing are for use with PIV-I smart cards. The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Level 4 Certificates except where specifically noted herein. PIV-I Content Signing policy is reserved for certificates used by the Card Management System (CMS) to sign the PIV-I card security objects.

This CP is only one of several documents that govern the DigiCert PKI. Other important documents include both private and public documents, including but not limited to Certification Practice Statements, registration authority agreements, subscriber agreements, relying party agreements, customer agreements, privacy policies, and memoranda of agreement. DigiCert may publish additional certificate policies or certificate 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 (9) 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). Revisions of this document have been made as follows:

Date	Changes	Version
26-August-2010	Updated the process used to authenticate the certificate requester's authority under section 3.2.5 for code signing	4.01

Date	Changes	Version
	certificates issued to organizations	
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
Root CA Certificates	2.16.840.1.114412.100
Intermediate CA Certificates	2.16.840.1.114412.200
Organization-Vetted SSL Certificates	2.16.840.1.114412.1
Extended Validation SSL Certificates	2.16.840.1.114412.2
Code Signing Certificates	2.16.840.1.114412.3
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	2.16.840.1.114412.4.3
Level 4 Certificates	2.16.840.1.114412.4.4
PIV-I Hardware - keys require activation by the PIV-I Cardholder (PIV Auth, Dig Sig and Key Management)	2.16.840.1.114412.5.1
PIV-I Card Authentication - keys do not require PIV-I Cardholder activation	2.16.840.1.114412.5.2
PIV-I Content Signing – use by PIV-I-compliant CMS	2.16.840.1.114412.5.3
EU Qualified Certificates	2.16.840.1.114412.6.1
EU QC on Secure Signature Creation Device	2.16.840.1.114412.6.2
Trusted Timestamping	2.16.840.1.114412.7.1
EQ Qualified Timestamping	2.16.840.1.114412.7.2

This CP applies to any entity asserting any of the OIDs identified above.

Subsequent revisions to this CP might have new OID assignments.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities ("Issuer CAs")

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 Board of Directors. 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, European Directive 99/93, CAB 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." In accordance with EU Directive 1999/93, EU Qualified Certificates will only be issued by Issuer CAs operated under the control of DigiCert. 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) 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 any applicable Registration Practices Statement under which the RA operates.

1.3.1. 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*.

1.3.2. 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.

1.3.3. Other Participants

When issuing PIV-I cards, the Issuer CA shall make a Card Management Systems (CMS) responsible for managing smart card token content. The Issuer CA shall ensure that the CMS meets the requirements described herein. The Issuer CA shall not issue any certificate to a CMS that includes a PIV-I Hardware or PIV-I Card Authentication policy OID. 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 *certificate*) 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.

This CP covers different types of end entity certificates/tokens with varying levels of assurance. The following table provides a brief description of the appropriate uses of each. The descriptions are for guidance only and are not binding.

Certificate/Token	Appropriate Use
OV SSL Certificates	Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
EV SSL Certificates	Used to secure online communication where risks and consequences

	of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.
Code Signing Certificates	Establishes the identity of the Subscriber named in the certificate and that the signed code has not been modified since signing.
Level 1 Client Certificates - Personal (email certificates)	Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.
Level 1 Client Certificates - Enterprise (C4 certificates)	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 2 Client Certificates (Corporate certificates)	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 3 Client Certificates (High assurance and FBCA Medium)	Used in environments where risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
Level 4 Client Certificates (Highest assurance and FBCA Medium Hardware)	Used in environments where risks and consequences of data compromise are high, including transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high. The requirements under this level of assurance also apply to PIV-I cards.
PIV-I Hardware PIV-I Card Authentication PIV-I Content Signing PIV-I Digital Signature PIV-I Key Management	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation PIN is not practical.
EU Qualified Certificate and EU QC on Secure Signature Creation Device	EU Qualified Certificates may only be used for signing (ETSI TS 101 456)
Time Stamp Token	Used to identify the existence of data at a set period of time.

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 free from malware, bugs, or vulnerabilities.

Certificates issued under this CP may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

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 200 - Canopy Building II

355 South 520 West
Lindon, UT 84042 USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481

1.5.2. Contact Person

Attn: Legal Counsel
DigiCert Policy Authority
Suite 200 - Canopy Building II
355 South 520 West
Lindon, UT 84042 USA

1.5.3. Person Determining CP 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 hereto. 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

"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.

"Application Software Vendor" means a software developer whose software displays or uses certificates and distributes root certificates.

"EU Directive 99/93" means the EU Council Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for Electronic Signatures, OJ L 13, 19.01.2000, pp. 12-20.

"EV Guidelines" is defined in section 1.1.

"Key Pair" means a Private Key and 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.

"**PIV-I Profile**" means the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Ver. 1.0, Date: April 23 2010.

"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 in Annex I of EU Directive 99/93 and is provided by an Issuer CA meeting the requirements of Annex II of the Directive.

"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 of an SSL Certificate prior to validating, relying on or using the SSL Certificate or accessing or using DigiCert's Repository. The Relying Party Agreement is available for reference at http://www.digicert.com/ssl-cps-repository.htm.

"Secure Signature Creation Device" means a signature-creation device that meets the requirements laid down in Annex III of the EU Directive 99/93.

"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, specific to a certificate type, that the Applicant for a certificate must read and accept before receiving a certificate.

"WebTrust" means the current version of the AICPA/CICA WebTrust Program for Certification Authorities.

Acronyms:

CA	Certificate Authority or Certification Authority
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCPA	DigiCert Policy Authority
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
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number (e.g. a secret access code)
PIV-I	Personal Identity Verification-Interoperable
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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

The Issuer CA shall publish its root certificate, 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

The Issuer CA shall make its repositories publically accessible on the web. Such public repositories shall include all root certificates, cross certificates, CRLs, CPs and CPSs.

2.3. TIME OR FREQUENCY OF PUBLICATION

The Issuer CA shall publish its CA certificates and CRLs as soon as possible after issuance, and any new or modified version of this CP, a CPS, or a standard Relying Party Agreement or Subscriber Agreement shall be published within seven days of its 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. 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.

Certificates for PIV-I cards must include both a non-null subject name and subject alternative name.

Each PIV-I Hardware certificate shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

cn=*Subscriber's full name*, ou=*Affiliated Organization Name*,{*Base DN*}

For certificates with no Affiliated Organization:

cn=*Subscriber's full name*, ou=Unaffiliated, ou=*Entity CA's Name*,{*Base DN*}

Each PIV-I Content Signing certificate shall clearly indicate the organization administering the CMS.

No PIV-I Card Authentication subscriber certificate shall include a Subscriber common name.

Each PIV-I Card Authentication certificate shall indicate whether or not the Subscriber is associated with an Affiliated Organization by taking one of the following forms:

For certificates with an Affiliated Organization:

serialNumber=*UUID*, ou=*Affiliated Organization Name*,{*Base DN*}

For certificates with no Affiliated Organization:

serialNumber=*UUID*, ou=Unaffiliated, ou=*Entity CA's Name*,{*Base DN*}

The UUID shall be encoded within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122 (e.g., "f81d4fae-7dec-11d0-a765-00a0c91e6bf6").

The subject name in EU Qualified Certificates must comply with section 3.1.2 of RFC 3739.

3.1.2. Need for Names to be Meaningful

When used, Distinguished Names in certificates shall identify both the subject and issuer of the certificate. Directory information trees shall accurately reflect organizational structures.

When User Principal Names (UPN) are used, they must be unique and accurately reflect organizational structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Where not otherwise prohibited by applicable policy (e.g. for certificate type, assurance level, or certificate profile), end-entity anonymous or pseudonymous certificates are not prohibited by this CP, as long as 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 that an Applicant's right to use a trademark be verified. However, the Issuer CA 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 Private Key for an EU Qualified Certificate stored on Secure Signature Creation Device (SSCD) shall be generated on the SSCD in the Subscriber's presence and secured by the Subscriber with PIN.

3.2.2. Authentication of Organization Identity

All organizational Applicants shall submit their name and address as part of the application process. The legal existence of all organizational Applicants shall be verified 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 such efforts are

insufficient to confirm the legal existence and identity of the subject, the Applicant may be required to provide legal documentation.

The authority of a person to request a certificate on behalf of an organization shall be verified in accordance with Section 3.2.5.

An Applicant's right to use any domain name(s) listed in an SSL certificate shall be verified through the registrar for that domain. Additional information required for issuance of EV Certificates shall be verified in accordance with the EV Guidelines.

For certificates that assert an organizational affiliation between a human subscriber and an organization (e.g. PIV-I Hardware Certificates), the organization shall enter into an agreement authorizing that affiliation and agreeing to request revocation of the certificate when that affiliation ends. See Sections 3.2.5, 4.9.1 and 9.6.1.

Also, all requests for Issuer CA certificates shall include the organization name, address, and documentation of the existence of the organization. The DCPA shall verify the information, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3.2.3. Authentication of Individual Identity

For the following certificate types, the Issuer CA or the 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 Server Certificate issued to an Individual	1. The Applicant must submit a legible copy of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). 2. Applicant name and address shall be cross-checked for consistency with reliable data sources. 3. If the Issuer CA or RA require further assurance, the Applicant shall be required to provide additional forms of identification, including non-photo and non-governmental identification such as recent utility bills, financial account statements, Applicant credit card, college/university ID, or equivalent document type. 4. The Issuer CA or RA shall confirm that it is able to communicate with the Applicant 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.
EV SSL Certificates issued to a Sole Proprietor	As specified in the EV Guidelines
Code Signing Certificate issued to an Individual	1. The Applicant must submit a legible copy of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). 2. Applicant name and address shall be cross-checked for consistency with reliable data sources. 3. If the Issuer CA or RA require further assurance, the Applicant shall be required to provide additional forms of

	identification, including non-photo and non-governmental identification such as recent utility bills, financial account statements, Applicant credit card, college/university ID, or equivalent document type. 4. The Issuer CA or RA shall confirm that it is able to communicate with the Applicant 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.
Level 1 Client Certificates – Personal (email certificates) (Equivalent to NIST 800-63/Kantara Level 1 and FBCA CP Rudimentary)	Applicant's control over an email address (or any of the identity verification methods listed below).
Level 1 Client Certificates - Enterprise (email certificates) (Equivalent to Citizen & Commerce Class Common CP (C4) Assurance Level-2.16.840.1.101.3.2.1.14.2)	Any one of the following: 1. In-person appearance before an RA or Trusted Agent with presentment of an original or certified government-issued 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 of the methods listed below.
Level 2 Client Certificates (Corporate certificates) (Equivalent to NIST 800-63/Kantara Levels 2 and 3 and FBCA CP Basic)	1. In-person proofing before an RA or Trusted Agent with presentment of a government-issued photo ID, examined for authenticity and validity. An entity certified by a State or National Government as being authorized to confirm identities may also perform in-person authentication on behalf of the RA, provided that the certified entity forwards the information collected from the applicant directly to the RA in a secure manner. 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. 2. Remotely verifying information provided by applicant (including name, date of birth, and current address or telephone number) through confirming his/her attestation to current possession of a government-issued photo ID and one additional form of ID such as another government-issued ID, an employee or student ID card number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. The Issuer CA or RA shall verify that the asserted name matches: (a) the referenced photo-ID; (b) date of birth; and (c) current address or personal telephone number; and are consistent with the application and sufficient to identify a unique individual. Confirmation of (c) may be obtained by issuing credentials in a manner that confirms: the address of record supplied by the applicant, or the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice. Additional information may be requested so as to ensure a unique identity, and alternative information may be sought if it leads to at least the same degree of certitude when verified. 3. Where the Issuer CA or RA has a current, ongoing relationship with the Applicant, identity may be verified through the 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, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods listed below.
Level 3 Client Certificates (Equivalent to NIST 800-63/Kantara Level 3, FBCA CP Medium, and EU Qualified 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). Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., driver's license). Credentials shall be examined for authenticity and validity. For each Level 3 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 information provided (name, date of birth, and current address) shall be verified to ensure legitimacy and may be 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, current address of record, and other personal information sufficient to ensure a unique identity. A trust relationship between an RA or Trusted Agent and the applicant that is based on an in-person antecedent (as defined in FBCA Supplementary Antecedent, In-Person Definition) may suffice as meeting the in-person identity proofing requirement provided that (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. If the photo ID is valid 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 Level 3 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) (Equivalent to NIST 800-63/Kantara Level 4, FBCA CP Medium Hardware, and EU Qualified Certificates utilizing Secure Signature Creation Devices) 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). Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., driver's license). Contemporaneous collection of at least one biometric (e.g. photograph or fingerprints) from the Applicant to ensure he or she cannot repudiate the application. Credentials shall be examined for authenticity and validity. For each Level 4 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. For Level 4 Client Certificates the use of an in-person antecedent is not applicable and identity shall be established no more than 30 days prior to initial certificate issuance. Level 4 Client Certificates shall be issued in a manner that confirms the Applicant's address of record.
PIV-I Certificates	PIV-I Hardware certificates shall only be issued to human subscribers. The following biometric data shall be collected by the RA or Trusted Agent during the identity proofing and registration process, which shall be formatted in accordance with [NIST SP 800-76] (see Appendix A): • An electronic facial image used for printing facial image on the card, as well as for performing visual authentication

	during card usage. The RA or Trusted Agent must collect a new facial image each time a card is issued; and • Two electronic fingerprints are stored on the card for automated authentication during card usage. The RA or Trusted Agent shall also require two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable and identity shall be established no more than 30 days prior to initial certificate issuance.
EU Qualified Certificates	Verify (in person) at time of registration by appropriate means in accordance with national law, the identity and, if applicable, any specific attributes of the person to whom the qualified certificate will be issued. Evidence of identity shall be checked against a physical person either directly or shall have been checked indirectly using means which provides equivalent assurance to physical presence. Submitted evidence may be in the form of either paper or electronic documentation. Where the subject is an individual, evidence provided shall consist of the person's passport or government-issued ID card and information collected shall include: full name (including surname and given names consistent with the applicable law and national identification practices); date and place of birth; and a nationally recognized identity number (or another attribute that distinguishes the person from others with the same name).

* 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,
  c. a unique identifying number from the verifier's identification,
  d. a unique identifying number from the Applicant's identification,
  e. the date and time of the verification, and
  f. a declaration of identity by the Applicant that is signed in handwriting 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.

If an Applicant cannot participate in face-to-face registration, a trusted person who already has a certificate of the same type applied for by the Applicant may represent the Applicant during the validation process. The trusted person must present their certificate and the Applicant's information to the person performing the face-to-face registration.

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 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). If the certificate is a pseudonymous certificate that identifies subjects by their organizational roles, then the Issuer CA shall validate 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

For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not desired, a certificate may be issued that corresponds to a Private Key that is shared by multiple Subscribers. The Issuer CA or the 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 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).

3.2.3.3. Authentication of Devices for Client Certificates

An Issuer CA may issue a Level 1, 2, 3 or 4 Client Certificate for use on a computing or network device, provided that the entity owning the device is listed as the subject. In all 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 client certificate's sponsor is changed, 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 in accordance with the requested client 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

For Level 1 - Personal client certificates verified only by email address, the Issuer CA shall not be required to confirm that the common name requested by the Applicant is the legal name of the

Subscriber, and such certificates shall contain a notice advising potential relying parties that the person's identity has not been verified. OV SSL Certificates may contain a pseudo-domain for use within the Subscriber's internal, non-public-DNS networks. Provided that the right to use a domain name is verified in accordance with Section 3.2.2, the Issuer CA may rely on the Subscriber's indication of the server or host name to issue a certificate containing the fully qualified domain name that includes the server or host name. 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, PIV-I, or EU Qualified certificate.

3.2.5. Validation of Authority

The authority of an individual requesting a certificate shall be verified as follows:

Certificate	Verification
OV Certificates	Verifying the authority of the requester with an authorized contact listed with the Domain Name Registrar (including WHOIS information), through a person with control over the domain, or though an out-of-band confirmation with the organization.
EV Certificates	Verifying authority of the Contract Signer and Certificate Approver in accordance with the EV Guidelines.
Code Signing Certificates	Confirming the contact information and authority of the certificate requester with an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication; and Obtaining approval of the certificate request using a means of communication confirmed by the organization
Level 1 Client Certificates - Personal (email certificates)	Verifying that the individual has control over the email address listed in the certificate.
Level 1 Client Certificates - Enterprise (email certificates)	Verifying the individual's certificate request with a person who has technical or administrative control over the domain name and verifying the requester's control over the email address listed in the certificate.
Client Certificates Levels 2, 3 and 4 and PIV-I Certificates	Verifying that the individual possesses evidence of an affiliation with the organization; confirming affiliation with the organization and the individual's authority to possess a certificate indicating such affiliation; and obtaining the organization's agreement that it will request revocation of the certificate when that affiliation ends.
EU Qualified Certificates	Verifying, in addition to sections 3.2.2 and 3.2.3, that the individual is associated with the organization and is authorized and that the organization consents to the publication of the certificate (see section 7.3.1 of TS 101 456).

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 and Code Signing Certificates to authenticate themselves with over 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
OV Certificates	Username and password	At least every six years
EV Certificates	Username and password	According to the EV Guidelines
Code 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	Shared secret (PIN/password) meeting NIST 800-63 Level 2 entropy requirements (Table A.2)	At least every nine years
Level 3 and 4 Client Certificates and PIV-I Certificates	Current signature key only	At least every nine years

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

After a certificate has been revoked other than during a renewal or update action, the Subscriber shall go through the initial registration process (described in Section 3.2) to obtain a new certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

All revocation requests shall be authenticated by the Issuer CA that issued the certificate or the RA that approved certificate issuance. Any revocation request may be authenticated by reference to 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

The DCPA shall establish requirements for who may 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

Validation personnel of the Issuer CA or the RA are responsible for verifying the identity of individual or entity in accordance with this CP prior to authorizing issuance of a certificate. Each Applicant shall submit sufficient information and documentation for the Issuer CA or the RA to perform the required verification of identity prior to issuing a Certificate. All communication during the certificate application process, including delivery of public keys to be included in Certificates, shall be authenticated and protected from modification.

4.2. CERTIFICATE APPLICATION PROCESSING

The Issuer CA or the RA shall verify the information in each certificate application and that proposed certificate contents are accurate prior to issuing the certificate.

4.2.1. Performing Identification and Authentication Functions

Validation personnel of the Issuer CA or the RA shall identify and verify each Applicant in accordance with Section 3.2. Applicable Certification Practice Statements and Registration Practice Statements must identify who (RA, Trusted Agent, other entity, or individual) performs the identification and authentication steps required to issue a Certificate to the Applicant in each case.

4.2.2. Approval or Rejection of Certificate Applications

Certificate applications that cannot be verified shall be rejected. The Issuer CA may also reject a certificate application on any reasonable basis, including the potential for issuance of the certificate to cause damage to business or reputation. There is no obligation for the Issuer CA to disclose its reasons for rejecting a certificate application.

Each Issuer CA and each RA shall follow industry standards when approving and issuing certificates. Subscribers are contractually obligated 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 can be established no more than 30 days before initial issuance of Level 3 and 4 and PIV-I Certificates.)

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

During the certificate issuance process, the Issuer CA shall verify that the identified and authenticated Applicant is the source of the certificate request and that the Applicant is the individual or entity that will be issued the Certificate. Databases used to confirm Subscriber identity information shall be protected from unauthorized modification or use. CA actions during the certificate issuance process shall be performed in a secure manner.

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

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.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

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.

4.4.2. Publication of the Certificate by the CA

All CA certificates shall be published to the Issuer CA's repository. The Issuer CA shall publish each Certificate by delivering it to the Subscriber.

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 as specified in the key usage extension of the corresponding Certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Party software shall be 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 name and attributes are unchanged, 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. After a client certificate is renewed, the old certificate may or may not be revoked but must not be further re-keyed, renewed, or modified.

4.6.2. Who May Request Renewal

Only an authorized representative of a Subscriber may request renewal of the Subscriber's certificates. An Issuer CA may renew a certificate without a corresponding request if the signing certificate is re-keyed.

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

All CA certificates shall be published to the Issuer CA's repository. The Issuer CA shall publish each Certificate by delivering it to the Subscriber.

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 be assigned a different validity period, key identifiers, specify different CRL and OCSP distribution points, and/or be signed with a different key.

Subscribers seeking re-key of Client Certificates shall identify themselves for the purpose of re-keying through use of their current signature key as permitted by Section 3.3.1. Subscribers of other types of certificates shall identify and authenticate themselves as stated in the applicable CPS.

After re-keying a client certificate, the Issuer CA may revoke the old certificate but shall not further re-key, renew, or modify the old certificate.

4.7.2. Who May Request Certificate Rekey

The Issuer CA may initiate certificate re-key at the request of the certificate subject or in its own discretion.

4.7.3. Processing Certificate Rekey Requests

The Issuer CA may require revalidation of the Subscriber prior to rekeying a certificate. At a minimum, the Issuer CA shall comply with section 3.3.1 in identifying the Subscriber 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 actual use of the certificate, constitutes the Subscriber's acceptance of it.

4.7.6. Publication of the Issued Certificate by the CA

All CA certificates shall be published to the Issuer CA's repository. The Issuer CA shall publish each Certificate by delivering it to the Subscriber.

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. Additional examples of circumstances when certificate modification may occur include minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures, organizational name change (e.g. as the result of merger, acquisition, or legally documented name change), and the replacement of the certificate where a minor error in certificate information or profile has been discovered.

After modifying a client certificate, the Issuer CA may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.8.2. Who May Request Certificate Modification

The Issuer CA may modify certificates 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

All CA certificates shall be published to the Issuer CA's repository. The Issuer CA shall publish each Certificate by delivering it to the Subscriber.

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 may revoke any certificate, in its sole discretion, including if it believes 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;
4. The Subscriber or the Issuer CA breached a material obligation under the CP, the CPS, or the relevant Subscriber 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 certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
7. The Issuer CA received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. The Issuer CA ceased operations and did not arrange for another certificate authority to provide revocation support for the certificate;
9. 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);
10. A court or arbitrator revoked the Subscriber's right to use a name or mark listed in the certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
11. Any information appearing in the Certificate was or became inaccurate or misleading;
12. 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
13. 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 always 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.

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 and 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 will 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. 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.

Whenever a PIV-I Card is no longer valid, the RA responsible for its issuance or maintenance shall collect it from the Subscriber as soon as possible, destroy it, and log its collection and physical destruction.

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. DigiCert provides revocation grace periods to Subscribers on a case-by-case basis. 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. All other subscribers are required to report key compromise and request revocation promptly but in no case later than 24 hours after discovery of a suspected compromise of their private key.

4.9.5. Time within which CA Must Process the Revocation Request

An Issuer CA shall revoke a certificate within one hour of receiving instruction from the DCPA to revoke a certificate. 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.

Other certificates shall be revoked as quickly as practical after validating the revocation request in accordance with the following process:

1. Revocation requests received two or more hours before a CRL issuance are processed before the next CRL is published,
2. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published, and

3. Regardless, all Certificate revocation requests are processed within 18 hours after their receipt.

4.9.6. Revocation Checking Requirement for Relying Parties

Prior to relying on 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

All Issuer CAs that operate offline and only issue CA certificates, certificate-status-checking certificates, or internal administrative certificates shall publish a CRL at least every 6 months (every 31 days for offline CAs chaining to the Federal Bridge CA). All other Issuer CAs shall publish CRLs at least every 24 hours (and within 18 hours of notice of a key compromise).

4.9.8. Maximum Latency for CRLs

The Issuer CA shall post an irregular, interim or emergency CRL to its online repository within four hours of generation (and no later than 18 hours after notification of compromise) and shall publish all regularly scheduled CRLs prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

An 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. An Issuer CA shall support online status checking via OCSP for all PIV-I certificates. Where offered, OCSP response times shall be no longer than six seconds.

4.9.10. On-line Revocation Checking Requirements

A relying party must 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 also use other methods to publicize the certificates it has revoked, 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.

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
Subscribers may 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
CA Private Keys are never escrowed. An Issuer CA may escrow Subscriber key management keys to provide key recovery services. Escrowed Private Keys shall be encrypted and protected using at least the level of security that was used to generate and deliver the Private Key. Under no circumstances may a Subscriber signature key be held in trust by a third party.

Subscribers and other authorized entities may request recovery of an escrowed Private Key. Entities escrowing Private Keys must 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 that receives 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,
5. Not enter into any obligation to communicate its key recovery process or requests to the Subscriber or any third party, and
6. Not disclose escrowed keys or escrowed key-related information to any third party unless required to do so by law or the entity's internal policies.

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 CMS equipment containing a PIV-I Content Signing key) 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, remove, 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. CMS and External RA Systems

All physical control requirements under this Section 5.1 apply equally to any 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 customer support and vetting. 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. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of CA and RA operations. Senior management of the Issuer CA or the RA shall be responsible for appointing individuals to trusted roles.

The Issuer CA or RA shall only allow trusted roles to access a CMS after the persons fulfilling those roles have been authenticated using a method commensurate with issuance and control of PIV-I Hardware.

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. CA Officers – CMS, RA, Validation and Vetting Personnel

The CA 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 to activate the Issuer CA's Private Keys, generate a CA key pair, or backup 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 are required to 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. Individuals may only assume one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role.

Separation of duties may be enforced either by the CA equipment, or 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 an Officer role, assume both the Administrator and Auditor roles, or assume both the Auditor and Officer roles. No individual shall have more than one identity.

The Issuer CA and the RA shall ensure that the PIV-I identity proofing, registration and issuance process adheres to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV-I credential without the cooperation of another authorized person.

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 and the CPS. Issuer CA and RA personnel and management within the DigiCert PKI shall be selected on the basis of loyalty, trustworthiness, and integrity. All trusted roles for Issuer CAs issuing Client Certificates at Levels 3 and 4 and for PIV-I Certificates 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, Code Signing or Client Certificates at Levels 1 and 2.

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

Each person fulfilling a trusted role must undergo checks and identification 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. Background investigations must be performed by a competent independent authority that has the authority to perform background investigations. The Issuer CA or RA shall require ach individual to appear in-person before a trusted agent whose responsibility it is verify identity. The trusted agent must 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 highest education degree obtained must be verified regardless of the date awarded.

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 relates to the person's job functions and covers:

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

The Issuer CA shall maintain records of who received training and what level of training was completed. Validation Specialists must have the minimum skills necessary to satisfactorily perform validation duties before they are granted validation privileges.

The Issuer CA or RA involved with the operation of CMS shall ensure that all personnel who perform duties involving the CMS receive comprehensive training. The Issuer CA and RA 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 0 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 (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. All event records shall be made available to 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
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

Auditable Event
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
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA components

Auditable Event
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 more thoroughly investigate any anomalies or irregularities detected. The Issuer CA or RA shall make a summary of each 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. Audit logs are made 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 Issuer CA or RA shall consider suspending its operation 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,
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 certificate status change 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 for at least 10.5 years.

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. The Issuer CA shall not release archives except as requested by the DCPA

or as required by law. 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 a an Issuer CA chooses to back up its archive records, the Issuer CA 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.

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.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

The Issuer CA shall implement data backup and recovery procedures and shall develop a Disaster Recovery and/or Business Continuity Plan (DR/BCP). The Issuer CA's shall have redundant CA systems that are located at a separate, geographically diverse location and that are configured for automatic failover in the event of a disaster (Disaster Recovery / Mirror Site). The Issuer CA shall review, test, and update the DR/BCP and supporting procedures annually. If a disaster occurs, the Issuer CA shall reestablish operational capabilities as quickly as possible.

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 system back-ups on a daily 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 will 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

The Issuer CA shall establish a secure facility in at least one secondary 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 the Issuer CA's operations are ever 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 no successor CA exists, all relevant records of the Issuer CA shall be transferred to a government regulatory 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.

The Issuer CA shall generate cryptographic keying material on a FIPS 140 level 3 validated cryptographic module using multiple individuals acting in trusted roles. When generating keying material, the Issuer CA shall create auditable evidence to show that the Issuer CA enforced role separation and followed its key generation process. The Issuer CA shall have an independent third party auditor validate the execution of the key process by either witnessing the key generation or by examining the 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 to the Subscriber. The entity may deliver Private Keys to Subscribers electronically or on a hardware cryptographic module / SSCD. In all cases:

1. 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 store, 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.

6.1.5. Key Sizes

The Issuer CA shall follow the NIST timelines in using and retiring signature algorithms and key sizes. The Issuer CA shall generate and use the following keys, signature algorithms, and hash algorithms for signing certificates, CRLs, and certificate status server responses:

2048-bit RSA Key with Secure Hash Algorithm version 1 (SHA-1)
2048-bit RSA Key with Secure Hash Algorithm version 2 (SHA-256)
384-bit ECDSA Key with Secure Hash Algorithm version 2 (SHA-256)

The Issuer CA may issue end-entity certificates that contain the following:

1. For certificates that expire on or before Dec 31, 2010, at least 1024-bit Public Keys for RSA or 224-bit Public Keys for ECDSA,
2. For certificates that expire on or after Dec 31, 2013 and that include a keyUsage extension that only asserts the digitalSignature bit, at least 2048 bits for RSA or DSA, or 224 bits for elliptic curve algorithms,
3. For certificates expiring after 12/31/2010, at least 2048 bits 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. The Issuer CA shall only issue end-entity certificates associated with PIV-I Cards that contain public keys and algorithms that conform to [NIST SP 800-78].

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. Signatures on certificates, OCSP responses, and CRLs that are issued after 12/31/2010 shall be generated using, at a minimum, SHA-224. Signatures on certificates, OCSP responses, and CRLs that are issued after 12/31/2030 shall be generated using, at a minimum, SHA-256.

The Issuer CA and Subscribers may fulfill their requirements under the CP and CPS using TLS or another protocol that provides similar security, provided the protocol requires at least:

1. triple-DES or equivalent for the symmetric key and at least 1024 bit RSA or equivalent for the asymmetric keys through 12/31/2010,
2. AES (128 bits) or equivalent for the symmetric key and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010, and
3. AES (128 bits) or equivalent for the symmetric key, and at least 3072 bit RSA or equivalent for the 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 Issuer CA shall set key usage bits or assert extended key usage OIDs for each certificate type in accordance with the DigiCert Certificate Profiles document.

The Issuer CA shall not issue Level 3 and Level 4 certificates that are certified for both signing and encryption. Level 1 and Level 2 certificates may include a single key for use with encryption and signature in support of legacy applications. 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.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

The Issuer CA shall use cryptographic hardware modules validated to FIPS 140 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
Level 1	N/A	FIPS 140 Level 1 (Hardware or Software)

Level 2	FIPS 140 Level 1 (Hardware or Software)	FIPS 140 Level 1 (Hardware or Software)
Level 3	FIPS 140 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Level 4 & PIV-I Card Authentication	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
EU QC on SSCD	EAL 4 Augmented (Hardware)	EAL 4 Augmented (Hardware)

The Issuer CA shall maintain any Card Management Master Key and perform diversification operations in a FIPS 140-2 Level 3 Cryptographic Module that conforms to [NIST SP 800-78]. The Issuer CA shall require PIV-I Hardware or commensurate to use the keys and shall require strong authentication of trusted roles when activating the Card Management Master Key. The Issuer CA shall also require that card management be configured such that only the authorized CMS can manage issued cards.

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 the 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 or dual use keys. The Issuer CA may escrow Subscriber Private Keys used for encryption.

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 backup (1) Level 1, Level 2, and Level 3 subscriber private signature keys, provided that the backup copies are held in Subscriber's control, and (2) subscriber key management keys. The Issuer CA may not backup Level 4 subscriber private signature keys. Backed up keys are never stored 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.

The Issuer CA may require backup of PIV-I Content Signing private signature keys to facilitate disaster recovery, provided that all backup is performed under multi-person control.

6.2.5. Private Key Archival

The Issuer CA shall not archive Private Keys. Private Keys associated with EU Qualified Certificates shall not be archived.

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

The Issuer CA 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
CRL and OCSP responder signing	3 years	31 days*
OV SSL	No stipulation	42 months
EV SSL	No stipulation	27 months
Time Stamping Authority	10 years	10 years
Code Signing Certificate	39 months	10 years†
Client used for signatures (including EU Qualified Certificates)	36 months	36 months
Client used for key management	36 months	36 months
Client for all other purposes	42 months	42 months
PIV-I Cards	60 months	60 months

* OCSP responder and CRL signing certificates associated with a PIV-I certificate may only have a maximum certificate validity period of 31 days.
† Extended from 39 months to 10 years under either the Time Stamp or Signing Authority method.

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.

PIV-I subscriber certificates may not expire later than the expiration date of the PIV-I hardware token on which the certificates reside.

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 signing root's 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 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.

6.4.3. Other Aspects of Activation Data

If the Issuer CA must reset activation data associated with a PIV-I certificate then a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3 is required. Either the Issuer CA or an RA must conduct this biometric 1:1 match.

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 privileges of users to 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 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. Hardware and software must be scanned 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 shall verify all software, when first loaded, as the unmodified software.

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 of manual procedures may be used to maintain system time. Clock adjustments are auditable events.

6.9. PIV-I CARDS

The following requirements apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards must use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
2. The Issuer CA shall ensure that all PIV-I Cards conform to [NIST SP 800-731].
3. The Issuer CA shall only issue the mandatory X.509 Certificate for Authentication under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. The Issuer CA shall only issue PIV-I certificates that conform to the PIV-I Profile.
5. The Issuer CA shall include an asymmetric X.509 Certificate for Card Authentication in each PIV-I card that:
    a. conforms to PIV-I Profile,
    b. conforms to [NIST SP 800-73], and
    c. is issued under the PIV-I Card Authentication policy.
6. The CMS shall include an electronic representation (as specified in SP 800-73 and SP 800-76) of the cardholder's facial image in each PIV-I card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. The CMS shall make its PIV-I Cards visual distinct from a Federal PIV Card to prevent creation of a fraudulent Federal PIV Card. At a minimum, the CMS shall not allow images or logos on a PIV-I Card to be placed within Zone 11, *Agency Seal*, as defined by [FIPS 201].
9. The CMS shall require the following items on the front of a card:
    a. Cardholder facial image,
    b. Cardholder full name,
    c. Organizational Affiliation, if exists; otherwise the issuer of the card, and
    d. Card expiration date.
10. The Issuer CA shall issue PIV-I cards with an expiration date that is five years or less.
11. All PIV-I Card must not expire later than the PIV-I Content Signing certificate on the card.
12. The Issuer CA shall include a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID in the digital signature certificate used to sign objects on the PIV-I Card. The PIV-I Content Signing certificate must conform to the PIV-I Profile.
13. The Issuer CA and its RAs shall manage the PIV-I Content Signing certificate and corresponding private key within a trusted Card Management System as defined herein.
14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.
15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall

meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78].

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

The Issuer CA shall issue X.509 version 3 certificates.

7.1.2. Certificate Extensions

The Issuer CA shall use certificate extensions in accordance with applicable industry standards, including RFC 3280/5280. The Issuer CA shall not issue certificates with a critical private extension.

PIV-I Certificates must comply with the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Date: April 23 2010, as set forth at: http://www.idmanagement.gov/fpkipa/documents/pivi_certificate_crl_profile.pdf.

7.1.3. Algorithm Object Identifiers

The Issuer CA 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 the 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 }

The Issuer CA 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 the Issuer CA issues a non-CA certificate for a federal agencies 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 }

Signature algorithms for PIV-I certificates are limited to those identified by NIST SP 800-78.

7.1.4. Name Forms

The Issuer CA shall use distinguished names that are composed of standard attribute types, such as those identified in RFC 3280/5280. The Issuer CA shall include a unique serial number in each certificate.

7.1.5. Name Constraints

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

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The Issuer CA shall use the OIDs listed in Section **Error! Reference source not found.** to identify its certificates and policies.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

The Issuer CA 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)

The Issuer CA shall issue version 2 CRLs that conform to RFC 3280/5280.

7.2.2. CRL and CRL Entry Extensions

The Issuer CA CRL extensions shall conform to the Federal PKI X.509 CRL Extensions Profile.

7.3. OCSP PROFILE

The Issuer CA shall operate an OCSP service in accordance with RFC 2560.

7.3.1. Version Number(s)

The Issuer CA 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 EV Guidelines and the AICPA/CICA WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188"). For Issuer CAs chained to the FBCA, the auditor letter of compliance shall meet the FPKIPA's Compliance Audit Requirements, dated October 28, 2009 (FPKIPA Audit Requirements).

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

On at least an annual basis, the Issuer CA shall retain an independent auditor who shall assess its 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

1. *Qualifications and experience*: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.

2. *Expertise*: The individual or group must be trained and skilled in the auditing of secure information systems and be familiar with Public Key infrastructures, certification systems, and Internet security issues.

3. *Rules and standards*: The auditor must conform to applicable standards, rules, and best practices promulgated by the American Institute of Certified Public Accountants (AICPA), the Canadian Institute of Chartered Accountants (CICA), the Institute of Chartered Accountants of England & Wales (ICAEW), the International Accounting Standards adopted by the European Commission (IAS), Information Systems Audit and Control Association (ISACA), the Institute of Internal Auditors (IIA), or another qualified auditing standards body.

4. *Reputation*: The firm must have a reputation for conducting its auditing business competently and correctly.

5. *Insurance*: EV auditors must maintain Professional Liability/Errors and Omissions Insurance, with policy limits of at least $1 million in coverage.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Issuer CA shall utilize an independent auditor that does 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.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports any 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 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. Where DigiCert operates a cross-certified Issuer CA or issues certificates under the authority of a government accrediting body, the DCPA shall notify the entity that cross-certified the Issuer CA Certificate or that relevant government accrediting body.

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.

8.7. SELF-AUDITS

The Issuer CA shall perform regular service quality audits against a randomly selected sample of certificates.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

The Issuer CA may charge fees for certificate issuance and renewal.

9.1.2. Certificate Access Fees

The Issuer CA may charge fees for access to its database 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

The Issuer CA 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
The Issuer CA shall specify what constitutes confidential information in its CPS.

9.3.2. Information Not Within the Scope of Confidential Information
Any information not listed as confidential information in the CPS is considered public information. Published certificate and revocation data is public information.

9.3.3. Responsibility to Protect Confidential Information
The Issuer CA's employees, agents, and contractors are responsible for protecting confidential information and are contractually obligated to do so. Employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan
The Issuer CA shall create and follow a privacy policy that specifies how the Issuer CA will handle personal information. The Issuer CA shall post the privacy policy on its website.

9.4.2. Information Treated as Private
The Issuer CA treats 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
Certificates, CRLs, and the personal or corporate information appearing in them are not considered private information.

9.4.4. Responsibility to Protect Private Information
All personnel involved with the DigiCert PKI are expected to handle personnel information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. The Issuer CA shall securely store and protect sensitive against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information
Personal data provided during the application, registration, and identity verification process that is not contained in Certificates is considered private information. An Issuer CA may only use private information with the subject's express written consent or as required by applicable law or regulation. Notwithstanding the foregoing, personal information contained in Certificates may be published in online public repositories. All Subscribers consent to the global transfer of any personal data contained in Certificates.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process
The Issuer CA 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

The Issuer CA shall not knowingly violate the intellectual property rights of any third party. The Issuer CA shall retain ownership over certificates but shall grant permission to reproduce and distribute certificates on a non-exclusive, royalty-free basis, provided that they are reproduced and distributed in full. Private Keys and Public Keys are the property of the Subscribers who rightfully issue and hold them.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

The Issuer CA represents that it complies, in all material aspects, with this CP, the CPS, its internal and published policies and procedures, and all applicable laws and regulations. The Issuer CA expressly disclaims all other representations except as otherwise stated in the CPS or in a separate agreement with a Subscriber.

For PIV, the Issuer CA shall maintain an agreement with Affiliated Organizations that includes obligations related to authorizing affiliation with Subscribers of PIV-I certificates.

9.6.2. RA Representations and Warranties

At a minimum, the Issuer CA shall require all RAs to represent that they have followed this CP and the CPS when participating in the issuance and management of certificates. The Issuer CA may include additional representations and obligations in its CPS or in its agreement with the RA.

9.6.3. Subscriber Representations and Warranties

The Issuer CA shall make Subscribers solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Prior to being issued a certificate, Subscribers shall contractually agree to:

1. Securely generate and protect their Private Keys from compromise,
2. Provide accurate and complete information and communication to the Issuer CA at all times,
3. Confirm the accuracy of certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify the Issuer CA if (i) any information that was submitted to the Issuer CA or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
5. Use the certificate only for authorized and legal purposes, consistent with this CPS and the relevant Subscriber Agreement, including only installing SSL 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,
6. Abide by the Subscriber Agreement and the CPS when requesting or using a Certificate, and
7. 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 provided for herein 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

An Issuer CA may limit its liability for each certificate type as set forth in its CPS. A CPS may exclude all liability for any certificate issued and managed in accordance with this CP and the CPS or in instances where a Subscriber or Relying Party has not complied with the terms and conditions of use for the Certificate.

9.9. INDEMNITIES

9.9.1. Indemnification by an Issuer CA

The Issuer CA's indemnification obligations are set forth in its CPS, Subscriber Agreement or Relying Party Agreement.

9.9.2. Indemnification by Subscribers

The Issuer CA shall include its indemnification requirements for Subscribers in the CPS and in its Subscriber Agreements.

9.9.3. Indemnification by Relying Parties

The Issuer CA shall include its indemnification requirements for Relying Parties in the 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, 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 or the CPS. Amendments are made by posting an updated version of the CP or CPS to the online repository. Controls are in place to reasonably ensure that this CP and the CPS is not amended and published without the prior authorization of the DCPA. The DCPA reviews this CP and the CPS annually.

9.12.2. Notification Mechanism and Period

The Issuer CA will post notice on its website of any proposed significant revisions to this CP. The notice will include a final date for receipt of comments and the proposed effective date. The Issuer CA does not have a fixed notice and comment period. The Issuer CA may make editorial and

typographical corrections, changes to contact details, and other changes that do not materially impact the parties without notice and without changing the version of this CP.

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 directive 95/46/EC 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

The Issuer CA shall contractually obligate every RA involved in Certificate issuance to comply with this CP and applicable industry Guidelines. The Issuer CA will also require parties using its products and services, such as Subscribers and Relying Parties, to accept agreements. No third party may rely on or bring action to enforce any such agreement.

9.16.2. Assignment

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

9.16.3. Severability

If any 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 any 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.