digicert®

FBCA Certification Practices Statement for EPCS and Other Programs

DigiCert, Inc.

Contents

1. INTRODUCTION

1.1. OVERVIEW

This Certification Practices Statement (CPS) defines the procedural and operational requirements that DigiCert, as an Entity CA of the Federal Bridge Certification Authority (FBCA) requires entities to adhere to when issuing and managing Certificates defined by and governed by the FBCA CP by the Federal Public Key Infrastructure Policy Authority (FPKI PA) and the DigiCert FBCA CP managed by the DigiCert Policy Management Authority (DCPA).

This document specifies the policies DigiCert adopts to meet the current versions of the following CPS:

Name of Policy/Guideline/Requirement Standard	Location of Source Document/Language
X.509 Certificate Policy for the Federal Bridge Certification Authority v.3.2	https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf
DigiCert FBCA CP for EPCS and Other Programs	https://www.digicert.com/legal-repository

The FBCA certificates issued through the DigiCert FBCA Intermediate CAs define trust through use of the policyMappings extension in the certificates.

Each policy defines an assurance level which refers to the strength of the binding between the public key and the subject of the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.

This CPS is only one of several documents that define the practices to meet the requirements of the DigiCert PKI for cross-certification with the FBCA. Other important documents include the FPKI Federal Bridge Certificate Policy, the DigiCert FBCA CP, trusted agent agreements and documentation, subscriber agreements, relying party agreements, customer agreements, privacy policies, and memoranda of agreement.

Where a specific practice is not stated, the requirements of the FBCA CP and DigiCert FBCA CP apply equally.

In this document, the term “device” means a non-person entity, i.e., a hardware device or software application.

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

1.1.1 FBCA Certificate Policy (CP)

FBCA certificates contain one or more registered certificate policy object identifiers (OID), which may be used by a relying party to decide whether a certificate is trusted for a particular purpose. Each OID corresponds to a specific level of assurance established by the FBCA Certificate Policy (CP).

1.1.2 Relationship between the FBCA CP and the DigiCert FBCA CP and CPS

This CPS states the practices to meet the requirements for the issuance and management of certificates issued by DigiCert as an Entity PKI in the FBCA program, and practices to meet the requirements for the operation of that FBCA cross-certification to maintain trust.

1.1.2.1 Relationship between the FBCA CP, DigiCert FBCA CP, and this CPS

This CPS is mapped to the FBCA that establishes criteria for cross-certification with DigiCert as an Entity CA and the DigiCert FBCA CP. The relationship between this CPS and those CPs are asserted in the policyMappings extension of the CA certificates issued to the Entity CA by the FBCA upon approval of the DigiCert FBCA CP. See section 1.2 for the DigiCert OIDs and the FBCA OIDs asserted in the policyMappings extension as specified in this CPS and the DigiCert FBCA CP.

1.1.3 Scope

DigiCert as an Entity CA of the FBCA is acting as part of that process by maintaining the practices that fulfill requirements to be approved for interoperability that allows DigiCert to facilitate the missions of the organizations. The generic term “entity” applies equally to Federal organizations and other organizations owning or operating PKI domains. As used in the FBCA CP, DigiCert as the Entity PKI or Entity CA may refer to an organization’s PKI, a PKI provided by a commercial service, or a bridge CA serving a community of interest.

1.2. DOCUMENT NAME AND IDENTIFICATION

This is the DigiCert X.509 Certification Practices Statement (CPS) for describing the practices that fullfill the requirements of interoperability to the Federal Bridge Certification Authority Certificate Policy and the DigiCert FBCA CP. This CPS is managed and approved by the DigiCert Policy Management Authority (DCPA). It was approved for publication on July 1st, 2024 and the table below specifies all revisions.

Version	Date	Change
1.0	July 1st, 2024	Initial document
1.1	July 15th, 2024	Add definitions and acronyms

DigiCert manages and maintains its OIDs in this repository, including the DigiCert-owned OIDs for this program: https://github.com/digicert/digicert_official_oids

OIDs in this CPS are included in Certificate Profiles for Certificates that must maintain the requirements of the mapped assurance levels in the FBCA CP and the DigiCert FBCA CP per this table:

Name	FBCA OIDs	Name	DigiCert OIDs
id-fpki-certpcy-basicAssurance	2.16.840.1.101.3.2.1.3.2	DigiCert Basic Assurance	2.16.840.1.114412.4.2
id-fpki-certpcy-medium-CBP	2.16.840.1.101.3.2.1.3.14	DigiCert Medium Assurance	2.16.840.1.114412.4.3.2
id-fpki-certpcy-mediumDevice	2.16.840.1.101.3.2.1.3.37	DigiCert Device	2.16.840.1.114412.1.11

1.3. PKI PARTICIPANTS

The following are roles relevant to the administration and operation of the DigiCert cross-certified bridge with the FBCA as an Entity CA:

1.3.1. PKI Authorities

1.3.1.1 DigiCert Policy Management Authority (DCPA)

DigiCert as a cross-certified Entity CA with the Federal Bridge CA is responsible for maintaining this CPS and for ensuring that all Entity PKI components are operated in compliance with the FBCA CP and DigiCert FBCA CP. Member PKIs in this program are operated comparably with the DigiCert FBCA CP through the practices described therein.

The DCPA or a DCPA appointed internal resource will notify the FPKIPA of any change to the infrastructure that has the potential to affect the FPKI operational environment at least two weeks prior to implementation; all new artifacts (CA certificates, Certificate Revocation List Distribution Point (CRLDP), Authority Information Access (AIA) and/or Subject Information Access (SIA) URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

1.3.2 Certification Authorities

The CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to Subscribers. DigiCert as the Entity CA is responsible for issuing and managing certificates including:

- The certificate manufacturing process
- Publication of certificates
- Revocation of certificates
- Generation and destruction of CA signing keys

- Ensuring that all aspects of the CA services, operations, and infrastructure related to certificates issued under the DigiCert FBCA CP are performed in accordance with the requirements, representations, and warranties of theDigiCert FBCA CP and the FBCA CP.

CA and related applications (e.g., OCSP, CMS, and KRS) may be hosted on one or more system software layers. Operational and technical security controls including audit logging requirements specified in the DigiCert FBCA CP and the FBCA CP applies to all system software layers, where appropriate and applicable. The specifics on those system specifications are explained in section 5 and 6.

1.3.2.1 Entity Cross-Certified Certification Authority (CA)

DigiCert designates at least one CA within its Entity PKI to receive a cross-certificate from the FBCA. This document refers to DigiCert as the Entity cross-certified CA. In addition, this CPS may refer to CAs that are "subordinate" to the DigiCert cross-certified CA. The use of the term "subordinate CA" encompasses any CA under the control of DigiCert that is subordinate to the cross-certified CA.

DigiCert's internal teams review and work with the FPKI to ensure that no CA under its PKI shall have more than one trust path to the FBCA during the application and issuance processes.

1.3.3 Card Management System (CMS)

No Stipulation.

No PIV-I credentials shall be issued from this program.

1.3.4 Registration Authorities

DigiCert operates as its own Registration Authority (RA). The RA is defined in the DigiCert FBCA CP as an entity authorized by DigiCert to collect, verify, and submit information provided by potential Subscribers for the purpose of issuing public key certificates. The term RA refers to hardware, software, and individuals that may collectively perform this function. Individuals fulfilling the RA function are acting in a Trusted Role.

The RA is responsible for:

- Control over the registration process.
- The identification and authentication process.

DigiCert also relies upon trusted agents to validate Applicants for FBCA Certificates. A Trusted Agent records information from and verifies biometrics (e.g., photographs) on presented credentials on behalf of the DigiCert RA for Applicants who cannot appear in person. Trusted Agents are not Trusted Roles.

1.3.5 Certificate Status Servers

DigiCert may optionally include an authority that provides status information about certificates on behalf of a CA through online transactions. DigiCert may include Online Certificate Status Protocol (OCSP) responders to provide online status information. Such an authority is termed a Certificate

Status Server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. Examples include OCSP servers that are identified in the AIA extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy.

1.3.6 Key Recovery Authorities

No stipulation.

1.3.7 Key Recovery Requestors

No stipulation.

1.3.8 Subscribers

A Subscriber is the entity whose name appears as the subject in a certificate. The term “Subscriber” as used in this CPS refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information. A Subscriber may be referred to as an "Applicant" after applying for a certificate, but before the certificate issuance procedure is completed.

1.3.9 Affiliated Organizations

No stipulation.

1.3.10 Relying Parties

A relying party is the entity that relies on the validity of the binding of the Subscriber’s identity to a public key. The relying party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information. The relying party can use the certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the holder of the certificate’s private key. A relying party may use information in the certificate (such as certificate policy identifiers, key usage, or extended key usage) to determine its appropriate usage.

For this CPS, the relying party may be any entity that wishes to validate the binding of a public key to the name of a Subscriber.

1.3.11 Other Participants

DigiCert may require the services of other security, community, and application authorities, such as compliance auditors.

1.4. CERTIFICATE USAGE

1.4.1. Appropriate Certificate Uses

Subscriber certificates issued by DigiCert in this CPS are used for several use cases including authentication, key management, signature, and confidentiality requirements. The sensitivity of the information processed or protected using certificates issued by DigiCert will vary significantly.

To provide sufficient granularity, DigiCert specifies security requirements from the FBCA CP at these different levels of assurance: Basic and Medium.

Relying Parties make risk-informed decisions when certificates are used to manage the identities of systems and users by evaluating the environment, associated threats, and vulnerabilities. This evaluation is done by the relying party and is not controlled by DigiCert or the FPKI. The following table provides additional guidance for determining which policy may be most appropriate based on the sensitivity of the information processed or protected using these certificates. These descriptions are intended as guidance and are not binding.

Basic: This level provides a basic level of assurance relevant to environments where there are risks and consequences of data compromise, but they are not considered to be of major significance. This may include access to private information where the likelihood of malicious access is not high. It is assumed at this security level that users are not likely to be malicious.

Medium: This level is relevant to environments where risks and consequences of data compromise are moderate. This may include transactions having substantial monetary value or risk of fraud, or involving access to private information where the likelihood of malicious access is substantial. This level of assurance includes the following certificate policies: Medium, Medium CBP, and Medium Device.

Federal relying parties should review more detailed guidance governing the use of electronic signatures (which include the use of digital certificates) issued by the Office of Management and Budget, as well as more detailed subordinate guidance issued by other agencies pursuant to OMB direction (such as NIST Federal Information Processing Standards and Special Publications).

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

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

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

1.5.2 Contact Person

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

Revocation Reporting Contact Person
Attn: Support
DigiCert Technical Support
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA
revoke@digicert.com

Subscribers or Relying Parties requiring assistance with revocation or an investigative report, see section 4.9 and the following publicly available webpage: https://problemreport.digicert.com/

If the problem reporting page is unavailable, there is a system outage, there are questions, or belief DigiCert findings are incorrect please contact revoke@digicert.com. Specifics of how DigiCert and the Trusted Agents under this program accept revocation requests are covered in section 4.9 of this CPS.

1.5.3 Person Determining CPS Suitability for the Policy

This DigiCert FBCA Certification Practices Statement conform to the corresponding DigiCert FBCA Certificate Policy. The process of this CPS conforming to the DigiCert FBCA CP will be evaluated by the DCPA prior to being approved for publication.

DigiCert designates the DigiCert Policy Management Authority (DCPA) that asserts that this CPS(s) conforms to the DigiCert FBCA CP.

In each case, the determination of suitability is based on a review by multiple internal teams, subject matter experts, and the DCPA voting members who review the material. Additional input provided an independent compliance auditor's results and recommendations are also taken into account by the DCPA upon completion of the annual audit. See Section 8 for further details.

1.5.4 CP Approval Procedures

The DCPA approves this CPS after the review specified in section 1.5.3 is completed and documents their approval for each version.

1.6 DEFINITIONS AND ACRONYMS

1.6.1 Definitions

Term	Definition
Applicant	An entity applying for a Certificate.
Certificate	An electronic document that uses a digital signature to bind a Public Key and an identity.
Certificate Management Process	Processes, practices, and procedures associated with the use of keys, software, and hardware, by which the CA verifies Certificate Data, issues Certificates, maintains a Repository, and revokes Certificates.
Direct Address	An email address conforming to the Applicability Statement for Secure Health Transport.
Direct Address Certificate	A Certificate containing an entire Direct Address.
Direct Organizational Certificate	A Certificate containing only the domain name portion of a Direct Address.
Domain Name	An ordered list of one or more Domain Labels assigned to a node in the Domain Name System.
Hardware Crypto Module	A tamper-resistant device, with a cryptography processor, used for the specific purpose of protecting the lifecycle of cryptographic keys (generating, managing, processing, and storing).
IP Address	A 32-bit or 128-bit number assigned to a device that uses the Internet Protocol for communication.
Key Compromise	A Private Key is said to be compromised if its value has been disclosed to an unauthorized person, or an unauthorized person has had access to it.
Key Pair	A Private Key and associated Public Key.
OCSP Responder	An online software application operated under the authority of DigiCert and connected to its repository for processing certificate status requests.
Private Key	The key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key	The key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key

	and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Relying Party	An entity that relies upon either the information contained within a Certificate or a time-stamp token.
Relying Party Agreement	An agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert's Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.
Subject Identity Information	Information that identifies the Certificate Subject. Subject Identity Information does not include a Domain Name listed in the subjectAltName extension or the Subject commonName field.
Subscriber	Either the entity identified as the subject in the Certificate or the entity that is receiving DigiCert's time-stamping services.
WebTrust	The current version of CPA Canada's WebTrust Program for Certification Authorities.
WHOIS	Information retrieved directly from the Domain Name Registrar or registry operator via the protocol, the Registry Data Access Protocol, or an HTTPS website.

1.6.2 Acronyms

Abbreviation	Meaning
CA	Certificate Authority or Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
DCPA	DigiCert Policy Authority
DNS	Domain Name Service
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HSM	Hardware Security Module

HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IDN	Internationalized Domain Name
IETF	Internet Engineering Task Force
ITU	International Telecommunication Union
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
TLD	Top-Level Domain
TLS	Transport Layer Security
TTL	Time To Live
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3 References

No stipulation

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 REPOSITORIES

The publicly accessible repository system is designed and implemented to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

2.2 PUBLICATION OF CERTIFICATION INFORMATION

2.2.1 Publication of Certificates and Certificate Status

CA and End Entity certificates contain only valid Uniform Resource Identifiers (URIs) that are publicly accessible.

DigiCert publishes all CA certificates it issues in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Subject Information Access (SIA) extension in all valid certificates issued to the CA. The file must be a certs-only Cryptographic Message Syntax file that has an extension of .p7c.

With the exception of self-signed certificates, all CA certificates are published by DigiCert in a file available via a publicly accessible HTTP URI. This URI must be asserted in the Authority Information Access (AIA) extension in all valid certificates issued by DigiCert.

DigiCert publishes the latest CRL covering all unexpired certificates via a publicly accessible HTTP URI until such time as all issued certificates have expired. This URI is asserted in the CRL distribution point extension of all certificates issued by that CA, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

A Certificate Status Server (CSS) provides status information about certificates on behalf of DigiCert through on-line transactions.

Pre-generated OCSP responses may be created by the CSS and distributed to OCSP servers. OCSP responses, like CRLs, are publicly distributable data. OCSP servers that lack OCSP response signing capability have the same security requirements as a repository hosting CRLs.

2.2.2 Publication of CA Information

This CPS, the DigiCert FBCA CP, and the annual PKI Compliance Audit Letter for the FBCA are publicly available online.

The DigiCert FBCA CP and the DigiCert FBCA CPS are available at: https://www.digicert.com/legal-repository

The annual PKI Compliance Audit Letter for this program is available at: https://www.digicert.com/webtrust-audits

2.3 TIME OR FREQUENCY OF PUBLICATION

This CPS and any subsequent changes are made publicly available within thirty (30) days of approval by the DCPA.

Publication requirements for CRLs are provided in Sections 4.9.7 and 4.9.12.

2.4 ACCESS CONTROLS ON REPOSITORIES

Repositories hosting CA certificates, CRLs, and pre-generated OCSP responsesare publicly accessible. Information not intended for public dissemination or modification is protected through redaction.

Posted certificates, CRLs, and pre-generated OCSP responses are replicated in additional repositories for performance enhancement when done.

3 IDENTIFICATION AND AUTHENTICATION

3.1 NAMING

3.1.1 Types of Names

CA certificates contain a non-null subject Distinguished Name (DN). All RA certificates include a non-NULL subject DN.

Naming requirements based on level of assurance are as follows:

Basic

- Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical.

Medium

- Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical.

3.1.1.1 Subject Names

Certificates issued to Subscribers include distinguished names that are comprised of a base distinguished name (Base DN) and additional relative distinguished names (RDNs).

DigiCert must define the permitted Base DN(s).

Device Subscriber distinguished names take the form of Base DN, CN=device name, where device name is a descriptive name for the device.

Role-based and group certificates are issued under human subscriber policy described in this CPS and the CP.

- Role-based certificates identify a specific role on behalf of which one or more subscribers are authorized to act rather than the subscriber's name. Where the organization is implicit in

the role, it should be omitted. Where the role alone is ambiguous, the organization must be present in the DN.

- The subjectName DN in a group certificate must not imply that the subject is a single individual, e.g., by inclusion of a human name form.

3.1.1.2 Subject Alternative Names

Subscriber certificates that contain id-kp-emailProtection in the EKU include a subject alternative name extension that includes a rfc822Name.

3.1.2 Need for Names to be Meaningful

Names used in the certificates issued by DigiCert identify the person or object to which they are assigned in a meaningful way.

The common name in the distinguished name represent the Subscriber in a way that is easily understandable for humans. For Human Subscribers, this will typically be a legal name.

When DNs are used, the directory information tree accurately reflect organizational structures.

When DNs are used, the common name respect name space uniqueness requirements and are not misleading. This does not preclude the use of pseudonymous certificates as defined in Section 3.1.3.

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

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

3.1.3 Anonymity or Pseudonymity of Subscribers

Subscriber certificates do not contain anonymous or pseudonymous identities.

DNs in subscriber certificates issued by DigiCert may contain a pseudonym (such as a large number) as long as name space uniqueness requirements are met.

DigiCert may issue group certificates that identify subjects by their organizational roles. Name space uniqueness requirements as described in 3.1.5 must be met.

3.1.4 Rules for Interpreting Various Name Forms

Distinguished Names in Certificates are interpreted using the X.500 series and ASN.1 syntax. E-mail addresses are interpreted using [RFC 5322].

3.1.5 Uniqueness of Names

DigiCert enforces name uniqueness within the X.500 namespace. Name uniqueness is not violated when multiple certificates are issued to the same entity.

3.1.6 Recognition, Authentication, and Role of Trademarks

DigiCert reserves the right to reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 INITIAL IDENTITY VALIDATION

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

3.2.1 Method to Prove Possession of Private Key

In all cases where the party named in a certificate generates its own keys that party proves possession of the private key that corresponds to the public key in the certificate request.

3.2.2 Authentication of Organization Identity

Prior to issuing a Certificate with Organizational information DigiCert will verify:

- The Organization has confirmed the subscriber is affiliated and has authorized the use of the Organization name in the Certificate;
- The Organization legally exists, maintains a physical address where it conducts business and a telephone number where its representatives can be contacted; and
- The authority of requesting representatives.

Certificates may also be issued to individuals who do not have affiliation to any organization and are acting in their personal capacity.

3.2.3 Authentication of Individual Identity

For each certificate issued, DigiCert must authenticate the identity of the individual requestor.

In addition to the processes described below, Subscriber certificates may be issued on the basisof an electronically authenticated request, using a valid signature or authentication certificate and associated private key, with the following restrictions:

- The assurance level of the new certificate must be the same or lower than the assurancelevel of the certificate used to authenticate the request;
- Identity information in the new certificate must match the identity information from thesignature or authentication certificate;
- The expiration date of the new certificate shall not exceed the next required initialidentity authentication date associated with the certificate used to authenticate therequest.
- The next required initial identity authentication date remains unchanged in the event of anew certificate issuance based on electronic authentication.

3.2.3.1 Authentication of Human Subscribers

For Subscribers, DigiCert ensures that the applicant's identity information is verified in accordance with the process established by the DIgiCert FBCA CP and this CPS. Process information depends upon the certificate level of assurance and is addressed in this CPS.

DigiCert as the CA and RA records the information set forth below for issuance of each certificate:

- The identity of the person performing the identification and either;
    - A signed declaration by that person that he or she verified the identity of the applicant as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.
    - An auditable record linking the authentication of the person performing the identification to their verification of each Applicant.
- If in-person or supervised remote1 identity proofing is done, a unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- If electronic authentication is done, a unique identifying number(s) from the signature or authentication certificate must be retained (e.g., certificate, serial number, thumbprint, SKI, public key, etc.)
- The date of the verification; and either:
    - An auditable record indicating the applicant accepted the certificate; or
    - A declaration of identity signed by the applicant using a handwritten signature or appropriate digital signature (see Practice Note) and performed in the presence of the person performing the identity authentication, 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 is unable to perform a required face-to-face, either in-person or supervised remote, registration (e.g., a network device), the applicant may be represented by a trusted person already issued a digital certificate by the Entity. The trusted person will present information sufficient for registration at the level of the certificate being requested, for both himself/herself and the applicant who the trusted person is representing.

An entity certified by a State or Federal Entity as being authorized to confirm identities may perform in-person authentication on behalf of DigiCert. The certified entity forwards the information collected from the applicant directly to DigiCert 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 DigiCert of its responsibility to verify the presented data.

Below are the identification requirements for each level of assurance covered by this CPS and required by the FBCA CP:

Basic

Identity may be established by in-person proofing before DigiCert or Trusted Agent; or remotely verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application and sufficient to identify a unique individual.

Address confirmation: * Issue credentials in a manner that confirms the address of record supplied by the applicant; or * Issue credentials in a manner that confirms the ability of the applicant to receive telephone communications at a number associated with the applicant in records, while recording the applicant's voice.

Medium

Identity must be established by in-person or supervised remote proofing before the DigiCert, a Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided must be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID2, or two Non-Federal Government I.D.s, one of which must be a photo I.D. Any credentials presented must be unexpired.

In addition to the above, a digital certificate of equal or greater assurance level as the new certificate may be used to assert identity. The existing digital certificate must be used for authentication of the holder and must contain user identity attributes identical to the new certificate (i.e., identical username).

If an applicant is denied a credential based on the results of the identity proofing process, DigiCert permits a mechanism for appeal or redress of the decision.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

Normally, a certificate is issued to a single Subscriber. For cases where there are several entities acting in one capacity, and where non-repudiation for transactions is not required, a certificate may be issued that corresponds to a private key that is shared by multiple Subscribers. DigiCert as the CA and RA records the information identified in Section 3.2.3.1 for a sponsor from the Information Systems Security Office or equivalent before issuing a group certificate.

In addition to the authentication of the sponsor, the following applies:

- The Information Systems Security Office or equivalent is responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The subjectName DN does not imply that the subject is a single individual, e.g., by inclusion of a human name form;
- The list of those with access to the shared private key is provided to, and retained by, DigiCert or its designated representative; and

3.2.3.4 Authentication of Devices

Some computing and communications devices (routers, firewalls, servers, etc.) will be named as certificate subjects. In such cases, the devices has hua human sponsor. The sponsor is responsible for providing the following registration information:

- Equipment identification (e.g., serial number) or service name (e.g., DNS name) or unique software application name
- Equipment or software application public keys
- Equipment or software application authorizations and attributes (if any are to be included in the certificate)
- Contact information to enable DigiCert to communicate with the sponsor when required

These certificates are issued only to devices under the issuing entity's control. In the case a human sponsor is changed, the new sponsor must review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. Sponsors are contractually obligated to notify DigiCert if the equipment is no longer in use, no longer under their control or responsibility, or no longer requires a Certificate. All registration is verified commensurate with the requested certificate type.

The registration information will be verified to an assurance level commensurate with the certificate assurance level being requested. For certificates issued with the id-fpki-certpcy-mediumDevice policies, registration information will be verified commensurate with the Medium assurance level.

Acceptable methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using certificates of equivalent or greater assurance than that being requested).
- In person or supervised remote registration by the sponsor, with the identity of the sponsor confirmed in accordance with the requirements of Section 3.2.3.1.

3.2.4 Non-verified Subscriber Information

All Subscriber information included in certificates is verified.

3.2.5 Validation of Authority

The organization named in the Certificate confirms to DigiCert that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.

3.2.6 Criteria for Interoperation

DigiCert does not have more than one intentional trust path to the FBCA.

3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1 Identification and Authentication for Routine Re-key

Subscribers of DigiCert identifies themselves for the purpose of re-keying through the following criteria from the FBCA CP:

Basic

- Identity may be established through use of current signature key, except that identity is reestablished through initial registration process at least once every 15 years from the time of initial registration.

Medium

- Identity may be established through use of current signature key, except that identity is established through initial registration process at least once every twelve years from the time of initial registration.
- For certificates asserting id-fpki-certpcy-mediumDevice, identity may be established through the use of the device's current signature key or the signature key of the device's human sponsor.

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 is required to go through the initial registration process described in Section 3.2 to obtain a new certificate, unless identity can be verified through the use of biometrics on file through the chain of trust defined in [FIPS 201].

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Revocation requests are authenticated. Requests to revoke a certificate may be authenticated using that certificate's public key, regardless of whether or not the associated private key has been compromised.

3.5 Identification and Authentication for Key Recovery Requests

No stipulation.

3.5.1 Third-Party Requestor Authentication

This section addresses the requirements for authentication of a Third-Party Requestor, i.e., a Requestor other than the Subscriber themself. The requirements for authentication, when the Requestor is the Subscriber, are addressed in Section 3.3.1 or Section 3.2.3.1.

Identity authentication is commensurate with the assurance level of the certificate associated with the key being recovered. Identity is established using one of the following methods:

- Procedures specified in Section 3.2.3 for authentication of an individual identity during initial registration for the specified certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).
- Certificate-based authentication (e.g., digitally signed e-mail or client-authenticated TLS) that can be verified using current, valid (i.e., un-revoked) public key certificates at the requested certificate policy assurance level (an assurance level equal to or greater than the assurance level of the certificate whose corresponding private key is being recovered).

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

The Certificate application process provides sufficient information to:

- Establish the Applicant's authorization by the employing or sponsoring agency to obtain a certificate. See Section 3.2.3 of this CPS and the FBCA CP for requirements.
- Establish and record the identity of the Applicant. See Section 3.2.3 of this CPS and the FBCA CP for requirements.
- Obtain the Applicant's public key and verify the Applicant's possession of the private key. See Section 3.2.3 of this CPS and the FBCA CP for requirements.
- Verify the information included in the certificate.

These steps may be performed in any order, but all must be completed before certificate issuance.

4.1.1 Who Can Submit a Certificate Application

Below is a list of people who may submit certificate applications:

- Any individual who is the subject of the certificate;
- Any authorized representative of an Organization or entity; or
- Any authorized representative of DigiCert

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. Applicants or individuals authorized to request Certificates, who are not included in any of the previous lists, may apply for a Certificate.

4.1.2 Enrollment Process and Responsibilities

All communications supporting the certificate application and issuance process is authenticated and protected from modification. Communications may be electronic or out-of-band.

Any electronic communication of shared secrets is protected.

Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair is used.

Subscribers are responsible for providing accurate information on their certificate applications.

If databases or other sources are used to confirm Subscriber attributes, then these sources and associated information sent to DigiCert is required to have an auditable chain of custody be in place when information is obtained through one or more information sources. All data received is protected and securely exchanged in a confidential and tamper evident manner and protected from unauthorized access.

4.2 CERTIFICATE APPLICATION PROCESSING

Information in certificate applications is verified as accurate before certificates are issued. The DigiCert FBCA CP and this CP must specify the procedures to verify the provided information.

4.2.1 Performing Identification and Authentication Functions

For DigiCert, the identification and authentication of the Subscriber meets the requirements specified for Subscriber authentication as specified in Sections 3.2 and 3.3 of this CPS and the FBCA CP. For DigiCert, as the CA and RA, the components of the Certificate application are verified in-house. Trusted Agents may be used to assist with the collection of Applicant information required by the DigiCert FBCA CP and through procedures described in this CPS, but DigiCert RA Agents are responsible for validation and verification of the information prior to issuance.

4.2.2 Approval or Rejection of Certificate Applications

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

DigiCert shall follow the requirements of this CPS and the FBCA CP when approving and issuing Certificates.

DigiCert shall contractually require subscribers to verify the information in a Certificate prior to using the Certificate.

4.2.3 Time to Process Certificate Applications

Certificate applications is processed and a certificate issued within 90 days of identity verification.

4.3 CERTIFICATE ISSUANCE

4.3.1 CA Actions during Certificate Issuance

Upon receiving the request, DigiCert:

- Verifies the identity of the requestor.

- Verifies the authority of the requestor and the integrity of the information in the certificate request.
- Verifies all attribute information received from a Subscriber before inclusion in a certificate.
- Builds and signs a certificate if all certificate requirements have been met.
- Makes the certificate available to the Subscriber after confirming that the Subscriber has formally acknowledged the obligations described in Section 9.6.3 of the FBCA CP and this CPS.

4.3.2 Notification to Subscriber by the CA of Issuance of Certificate

DigiCert shall notify the Subscriber within a reasonable time of certificate issuance and make the Certificate available to the Subscriber.

4.4 CERTIFICATE ACCEPTANCE

Before a Subscriber can make effective use of its Private Key, the Subscriber accepts the responsibilities defined in Section 9.6.3 of this CP by accepting the Subscriber agreement.

4.4.1 Conduct Constituting Certificate Acceptance

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

- Downloading a Certificate or installing a Certificate from a message attaching it constitutes the Subscriber's acceptance of the Certificate; or
- Failure of the Subscriber to object to the certificate or its content constitutes certificate acceptance.

4.4.2 Publication of the Certificate by the CA

No stipulation.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 KEY PAIR AND CERTIFICATE USAGE

4.5.1 Subscriber Private Key and Certificate Usage

The certificate shall be used lawfully in accordance with DigiCert's Subscriber Agreement the terms of this CPS and the DigiCert FBCA CP.

All Subscribers shall protect their Private Keys from unauthorized use or disclosure by third parties and shall use their Private Keys only for their intended purpose in accordance with section 9.6.3.

Restrictions in the intended scope of usage for a private key are specified through certificate extensions, including the key usage and extended key usage extensions, in the associated certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Relying Parties shall use software that is compliant with X.509 and applicable IETF PKIX standards. DigiCert 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 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 obtains such assurances before using the Certificate.

4.6 CERTIFICATE RENEWAL

Renewing a certificate means creating a new certificate with a new serial number where all certificate subject information, including the subject public key and subject key identifier, remain unchanged.

The new certificate may have an extended validity period and may include new issuer information (e.g., different CRL distribution point, AIA and/or be signed with a different issuer key).

Once renewed, the old certificate may or may not be revoked, but is not reused for requesting further renewals, re-keys, or modifications.

4.6.1 Circumstance for Certificate Renewal

A certificate may be renewed if the public key has not reached the end of its validity period, the associated private key has not been compromised, and the Subscriber name and attributes are unchanged. In addition, the validity period of the certificate meets the requirements specified in Section 6.3.2 of this CPS and the FBCA CP.

CA certificates and Delegated OCSP responder certificates may be renewed so long as the aggregated lifetime of the private key does not exceed the requirements specified in Section 6.3.2 of this CP and the FBCA CP.

4.6.2 Who May Request Renewal

DigiCert requests renewal of cross-certificates from the FPKIMA.

For all other CA certificates and Delegated OCSP responder certificates, the corresponding operating authority may request renewal.

Subscriber renewal requests is accepted only from certificate subjects, PKI sponsors, or DigiCert RA Agents. Additionally, DigiCert may perform renewal of its subscriber certificates without a corresponding request, such as when the CA re-keys.

4.6.3 Processing Certificate Renewal Requests

When DigiCert as a CA rekeys, it may renew the certificates it has issued.

When certificates are renewed as a result of CA key compromise, as described in Section 4.6.1, DigiCert verifies all certificates issued since the date of compromise were issued appropriately. If the certificate cannot be verified, then it is not renewed.

4.6.4 Notification of New Certificate Issuance to Subscriber

As specified in Section 4.3.2.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

As specified in Section 4.4.1.

4.6.6 Publication of the Renewal Certificate by the CA

As specified in Section 4.4.2.

4.6.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.7 CERTIFICATE RE-KEY

Re-key is identical to renewal except the new certificate has a different subject public key (and serial number).

Subscribers of DigiCert identifies themselves for the purpose of re-keying as required in Section 3.3.1 of this CP and the FBCA CP.

Once re-keyed, the old certificate may or may not be revoked, but is not reused for requesting further re-keys, renewals, or modifications.

4.7.1 Circumstance for Certificate Rekey

Circumstances requiring certificate re-key include nearing the maximum usage period of a private key, certificate expiration, loss or compromise, issuance of a new hardware token, and hardware token failure.

Section 6.3.2 establishes maximum usage periods for private keys for both CAs and Subscribers.

4.7.2 Who May Request Certification of a New Public Key

For DigiCert CA certificates and Delegated OCSP responder certificates, DigiCert may request re-key of its own certificate.

Subscribers with a currently valid certificate may request re-key of the certificate. DigiCert as the CA and RA may request certification of a new public key on behalf of a Subscriber. The human sponsor of a device may request re-key of the device certificate.

4.7.3 Processing Certificate Rekey Requests

Before performing re-key, DigiCert identifies and authenticates the requestor by performing the identification processes defined in Section 3.2 or Section 3.3 of this CP and the FBCA CP. Digitally signed Subscriber re-key requests is validated before the re-key requests are processed.

4.7.4 Notification of Certificate Rekey to Subscriber

As specified in Section 4.3.2.

4.7.5 Conduct Constituting Acceptance of a Rekeyed Certificate

As specified in Section 4.4.1.

4.7.6 Publication of the Rekeyed Certificate by the CA

As specified in Section 4.4.2.

4.7.7 Notification of Certificate Issuance by the CA to Other Entities

As specified in Section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Modifying a certificate means creating a new certificate that has the same or a different key and a different serial number, and that differs in one or more other fields from the old certificate. Once modified, the old certificate may or may not be revoked, but is not reused for requesting further renewals, re-keys, or modifications.

4.8.1 Circumstance for Certificate Modification

CA certificates and Delegated OCSP responder certificates whose characteristics have changed (e.g., assert new policy OID) may be modified. The new certificate may have the same or a different subject public key.

A certificate associated with a Subscriber whose characteristics have changed (e.g., name change due to marriage) may be modified. The new certificate has a different subject public key.

4.8.2 Who May Request Certificate Modification

DigiCert may request certificate modification for current cross-certificates. For DigiCert CA certificates and Delegated OCSP responder certificates, DigiCert may request modification.

Subscribers with a currently valid certificate may request modification of the certificate. The human sponsor of a device may request modification of the device certificate. DigiCert as the CA and RA may request certificate modification on behalf of a Subscriber.

4.8.3 Processing Certificate Modification Requests

DigiCert may request modification of its CA and cross-certified certificates to the FPKIMA for the following reasons:

- Modification of SIA extension; or
- Minor name changes (e.g., change CA1 to CA2) as part of key rollover procedures.

Proof of all subject information changes is provided to DigiCert or other designated agent and verified before the modified certificate is issued. If the modified certificate is issued with a new (different) public key, the additional requirements specified in Section 4.7.3 also applies.

If an individual's authorizations or privileges change, such that the modified certificate indicates a reduction in privileges and authorizations, the old certificate will be revoked.

4.8.4 Notification of Certificate Modification to Subscriber

As specified in Section 4.3.2.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

As specified in Section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

As specified in Section 4.4.2.

4.8.7 Notification of Certificate Modification by the CA to Other Entities

As specified in Section 4.4.3.

4.9 CERTIFICATE REVOCATION AND SUSPENSION

Revocation requests are authenticated. Requests to revoke a certificate may be authenticated using that certificate's associated private key, regardless of whether or not the private key has been compromised.

For Medium, and Basic Assurance, DigiCert will publish CRLs.

DigiCert will notify the FPKIPA at least two weeks prior to the revocation of a CA certificate, whenever possible. For emergency revocation, DigiCert follows the notification procedures in Section 5.7 of this CPS and the FBCA CP.

4.9.1 Circumstances for Revocation

A certificate is revoked when the binding between the subject and the subject's public key defined within the certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- Identifying information or affiliation components of any names in the certificate becomes invalid. Examples include

    - Subscriber no longer affiliated with sponsoring entity
    - A wild card certificate has been issued with a name where PKI Sponsor does not exercise control of the entire namespace associated with the wild card certificate.
- Privilege attributes asserted in the Subscriber's certificate are reduced.
- The Subscriber can be shown to have violated the stipulations of its Subscriber agreement.
- There is reason to believe the private key has been compromised.
- The Subscriber or other authorized party (as defined in the CPS) asks for his/her certificate to be revoked.
- The failure of DigiCert to adequately adhere to the requirements of the FBCA CP or the approved DigiCert FBCA CPS.

DigiCert , at a minimum, revokes certificates for the reason of key compromise upon receipt of an authenticated request from an appropriate entity.

For certificates that express an organizational affiliation, DigiCert requires that the organization inform DigiCert of any changes in the subscriber affiliation. If the affiliated organization no longer authorizes the affiliation of a Subscriber, DigiCert revokes any certificates issued to that Subscriber containing the organizational affiliation. If an organization terminates its relationship with DigiCert such that it no longer provides affiliation information, DigiCert revokes all certificates affiliated with that organization.

If it is determined that revocation is required, the associated certificate is revoked and placed on the CRL. Revoked certificates is included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

DigiCert may revoke certificates it has issued. Unless provided prior to revocation, notice and brief explanation for the revocation will subsequently be emailed to the Subscriber.

DigiCert or other authorized agency officials may request the revocation of a Subscriber's certificate.

DigiCert accepts revocation requests from subscribers, device sponsors. Affiliated Organization named in the certificate and third parties. Third party requests are limited to mis-issuance and mis-use of the certificate.

4.9.3 Procedure for Revocation Request

DigiCert revokes certificates upon receipt of sufficient evidence of compromise or loss of the subscriber's corresponding private key.

If it is determined that a private key used to authorize the issuance of one or more certificates may have been compromised, all certificates directly or indirectly authorized by that private key since the date of actual or suspected compromise is revoked or is verified as appropriately issued.

4.9.4 Revocation Request Grace Period

The revocation request grace period is the time available to the subscriber within which the subscriber makes a revocation request after reasons for revocation have been identified.

In the case of key compromise, DigiCert requests revocation within one hour of confirmation although the certificate may take longer to propagate on its respective CRL.

4.9.5 Time within which CA Must Process the Revocation Request

DigiCert will revoke subscriber certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests are processed before the next CRL is published, excepting those requests validated within two hours of CRL issuance. Revocation requests validated within two hours of CRL issuance is processed before the following CRL is published.

4.9.6 Revocation Checking Requirements for Relying Parties

Relying parties are expected to verify the validity of certificates as specified in [RFC 5280].

Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the Relying Party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

4.9.7 CRL Issuance Frequency

For this CPS, CRL issuance encompasses both CRL generation and publication.

CRLs are issued periodically, even if there are no changes to be made, to ensure timeliness of information.

For all other certificate assurance levels in this CP, online CRLs are set at a maximum interval for CRL issuance of every 24 hours.

4.9.8 Maximum Latency for CRLs

DigiCert publishes CRLs within 4 hours of generation.

Furthermore, each CRLis published no later than the time specified in the nextUpdate field of the previously issued CRL for same scope.

If pre-generation of CRLs is implemented, the thisUpdate field will be the date of generation. The nextUpdate value will be beyond the date of planned publication.

4.9.9 On-line Revocation Checking Availability

OCSP services are designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually, with resources sufficient to provide a response time of ten (10) seconds or less under normal operating conditions.

4.9.10 Online Revocation Checking Requirements

On-line revocation status checking is optional for relying parties. For certificates where revocation status online checking is not available, CRLs are used.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

DigiCert uses commercially reasonable efforts to notify potential Relying Parties if it discovers or suspects the compromise of a Private Key. DigiCert will transition any revocation reason code in a CRL to "key compromise" upon discovery of such reason or as required by an applicable CP.

Reports to DigiCert of key compromise must include:

- Proof of key compromise in either of the following formats:
    - A CSR signed by the compromised private key with the CommonName "Proof of Key Compromise for DigiCert"; or
    - The private key itself.
- If a CSR is provided, DigiCert will only accept proof of key compromise, if one of the following algorithms are used to sign the CSR:
    - SHA256WithRSA
    - SHA384WithRSA
    - SHA512WithRSA
    - ECDSAWithSHA256
    - ECDSAWithSHA384
    - ECDSAWithSHA512
    - SHA256WithRSAPSS
    - SHA384WithRSAPSS
    - SHA512WithRSAPSS
    - PureEd25519

DigiCert provides specific instructions and support for Key compromise on the following website: https://problemreport.digicert.com/ and other resources as indicated in section 1.5.2 of this CPS.

When a CA certificate is revoked or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, an emergency CRL is published based on the assurance level within the maximum latency time frames for emergency CRL Issuance listed below:

- Basic, within 24 hours after the notification.
- Medium within 18 hours after notification.

4.9.13 Circumstances for Suspension

No stipulation.

4.9.14 Who Can Request Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 CERTIFICATE STATUS SERVICES

No stipulation.

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 END OF SUBSCRIPTION

No Stipulation.

4.12 KEY ESCROW AND RECOVERY

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

CA equipment is protected from unauthorized access while the cryptographic module is installed and activated. DigiCert implements physical access controls to reduce the risk of equipment

tampering even when the cryptographic module is not installed and activated. CA cryptographic tokens is protected against theft, loss, and unauthorized use.

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

5.1.1 Site Location and Construction

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

5.1.2 Physical Access

The CA equipment, to include remote workstations used to administer the CAs, is always protected from unauthorized access. The security mechanisms commensurates with the level of threat in the equipment environment.

DigiCert adheres to the following security requirements:

- Ensure no unauthorized access to the hardware is permitted.
- Ensure all removable media and paper containing sensitive plain-text information is stored in secure containers.

The following requirements apply to DigiCert for issuing Medium certificates:

- Ensure manual or electronic monitoring for unauthorized intrusion at all times.
- Ensure an access log is maintained and inspected periodically.
- Require two-person physical access control to both the cryptographic module and computer systems.

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

A security check of the facility housing the CA equipment or remote workstations used to administer the CAs (operating at the Basic Assurance level or higher) occurs if the facility is to be left unattended. At a minimum, the check verifies the following:

- The equipment is in a state appropriate to the current mode of operation (e.g., that cryptographic modules are in place when “open”, and secured when “closed”; and for offline CAs, that all equipment other than the repository is shut down).
- Any security containers are properly secured.

- Physical security systems (e.g., door locks, vent covers) are functioning properly.
- The area is secured against unauthorized access.

A person or group of persons is made explicitly responsible for making such checks. When a group of persons is responsible, a log identifying the person performing a check at each instance is maintained. If the facility is not continuously attended, the last person to depart initials a sign-out sheet that indicates the date and time, and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.2.2 Physical Access for RA Equipment

DigiCert RA equipment is protected from unauthorized access while the cryptographic module is installed and activated. DigiCert implements physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. These security mechanisms commensurates with the level of threat in the RA equipment environment.

5.1.2.3 Physical Access for CSS Equipment

Physical access control requirements for CSS equipment that has signing capability meets the CA physical access requirements specified in Section 5.1.2.1. CSS equipment that does not have a private signing key and only distribute pre-generated OCSP responses are not required to meet these requirements.

5.1.3 Power and Air Conditioning

DigiCert has sufficient alternative power supply in the event of a primary power source failure to either maintain CA operations or, at a minimum, prevent loss of data. The repositories (containing CA certificates, CRLs, and pre-generated OCSP responses) is provided with uninterrupted power sufficient for a minimum of six (6) hours operation in the absence of commercial power, to maintain availability and avoid denial of service.

5.1.4 Water Exposures

CA equipment is installed such that it is not in danger of exposure to water (e.g., on tables or elevated floors).

Water exposure from fire prevention and protection measures (e.g., sprinkler systems) are excluded from this requirement.

5.1.5 Fire Prevention and Protection

DigiCert complies with local commercial building codes for fire prevention and protection.

5.1.6 Media Storage

Sensitive CA media is stored to protect it from accidental damage (water, fire electromagnetic) and unauthorized physical access.

5.1.7 Waste Disposal

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

5.1.8 Off-site Backup

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

For offline CAs, the backup is performed each time the system is turned on or once per week, whichever is less frequent.

Requirements for CA private key backup are specified in Section 6.2.4.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The personnel selected to fill these roles is extraordinarily responsible or the integrity of the CA is weakened. The functions performed in these roles form the basis of trust the entire PKI. Two approaches are taken to increase the likelihood that these roles can be successfully carried out. The first ensures that the person filling the role is trustworthy and properly trained. The second distributes the functions among more than one person, so that any malicious activity would require collusion.

The requirements of this policy are defined in terms of four roles; implementing organizations may define additional roles provided the following separation of duties are enforced.

1. Administrator – authorized to install, configure, and maintain the CA; establish and maintain system accounts; configure audit parameters; and generate PKI component keys.
2. Officer – authorized to request or approve certificate issuance and revocations.
3. Auditor – authorized to review, maintain, and archive audit logs.
4. Operator – authorized to perform system backup and recovery.

Administrators do not issue certificates to subscribers.

Separation of duties complies with Section 5.2.4, and requirements for two-person control with Section 5.2.2, regardless of the titles and numbers of Trusted Roles.

5.2.1.1 Registration Officers – CMS, RA, Validation and Vetting Personnel

The Registration Officer role is responsible for issuing and revoking Certificates.

5.2.2 Number of Persons Required per Task

Only one person is required per task for CAs operating at the Basic Levels of Assurance. Two or more persons are required for the follow DigiCert CAs for the following tasks:

- CA, key generation.
- CA signing key activation.
- CA, private key backup.

Where multiparty control is required, at least one of the participants will be an Administrator. All participants serve in a trusted role as defined in Section 5.2.1. Multiparty control for logical access will not be achieved using personnel that serve in the Auditor Trusted Role.

5.2.3 Identification and Authentication for each Role

At all assurance levels an individual will identify and authenticate him/herself before being permitted to perform any actions set forth above for that role or identity.

5.2.4 Roles Requiring Separation of Duties

Individual personnel is specifically designated to the four roles defined in Section 5.2.1 above. Individuals may assume only one of the Officer, Administrator, and Auditor roles, but any individual may assume the Operator role. The CA, CMS, and RA software and hardware identifies and authenticate its users and ensures 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 may have more than one identity.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles working on the DigiCert CA are selected on the basis of loyalty, trustworthiness, and integrity. Each person filling those specific trusted roles satifies at least one of the following:

- The person is a citizen of the country where DigiCert is located; or
- For PKIs operated on behalf of multinational governmental organizations, the person is a citizen of one of the member countries; or
- For PKIs located within the European Union, the person is a citizen of one of the member States of the European Union; or
- For RA personnel of DigiCert only, in addition to the above, the person may be a citizen of the country where the RA is located.

5.3.2 Background Check Procedures

DigiCert personnel receives a favorable adjudication after undergoing a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified.

Adjudication of the background investigation must be performed by a competent adjudication authority using a process consistent with [Executive Order 12968] or equivalent.

If a formal clearance is the basis for background check, the background refresh must be in accordance with the corresponding formal clearance. Otherwise, the background check must be refreshed every ten years.

5.3.3 Training Requirements

All designated Trusted Role personnel performing duties with respect to the operation of the CA or RA receives comprehensive training relevant to their duties. Training must be conducted in the following areas:

- Security principles and mechanisms;
- All PKI software versions in use on the system;
- All PKI duties they are expected to perform;
- Disaster recovery and business continuity procedures; and
- Stipulations of the Common CP, the Digicert FBCA CP and this CPS.

5.3.4 Retraining Frequency and Requirements

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

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

5.3.5 Job Rotation Frequency and Sequence

Job rotation will not violate role separation. All access rights associated with a previous role will be terminated.

All job rotations are documented. Individuals assuming an auditor role will not audit their own work from a previous role.

5.3.6 Sanctions for Unauthorized Actions

DigiCert takes appropriate administrative and disciplinary actions against personnel who have performed actions involving the CA or its RAs that are not authorized in this CP, CPS, or other documented procedures.

5.3.7 Independent Contractor Requirements

Contractors fulfilling Trusted Roles are subject to all personnel requirements stipulated in the corresponding policy.

PKI vendors who provide any services establishes procedures to ensure that any subcontractors perform in accordance with the DigiCert FBCA CP and this CPS.

5.3.8 Documentation Supplied to Personnel

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

5.4 AUDIT LOGGING PROCEDURES

The objective of audit log processing is to review all actions to ensure they are made by authorized parties and for legitimate reasons.

At a minimum, audit records are generated for all applicable events identified in Section 5.4.1 of the FBCA CP and this CPS and is available during audit reviews and third-party audits. For CAs operated in a virtual environment, audit records are generated for all applicable events on application software and all system software layers.

Where possible, the security audit logs are automatically collected. Where this is not possible, a logbook, paper form, or other physical mechanism must be used. All security audit logs, both electronic and non-electronic, must be retained and made available during compliance audits.

Audit record reviews should be performed using an automated process, and includes verification that the logs have not been tampered with, an inspection of log entries, and a root cause analysis for any alerts or irregularities. Implementation and documentation of automated tools describe relevant events and anomalies.

A record of the review, all significant events, and any actions taken as a result of these reviews are explained in an audit log summary. This review summary is retained as part of the long-term archive.

Real-time alerts are neither required nor prohibited by the FBCA CP and this CP.

5.4.1 Types of Events Recorded

All security auditing capabilities of CA operating system and CA applications required by the FBCA CP and this CPS are enabled during installation. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- What type of event occurred;
- Date and time when the event occurred;
- Where the event occurred (e.g., on what systems or in what physical locations);
- Source of the event;
- Outcome of the event to include success or failure; and
- Identity of any individuals, subjects, or objects/entities associated with the event.

Any request or action requiring the use of a private key controlled by the CA is an auditable event.

If out-of-band processes are used for authorization of certificate issuance, external artifacts from the process (e.g., forms, emails, etc.) will be recorded.

The CA records the events identified in the table below, where applicable to the application, environment, or both. Where these events cannot be electronically logged, electronic audit logs are supplemented with physical logs as necessary.

SECURITY AUDIT

Auditable Event	Basic	Medium
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X
Any attempt to delete or modify the Audit logs	X	X

IDENTIFICATION AND AUTHENTICATION

Auditable Event	Basic	Medium
The value of maximum authentication attempts is changed	X	X
The number of unsuccessful authentication attempts exceeds the maximum	X	X

Auditable Event	Basic	Medium
authentication attempts during user login		
An Administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts	X	X
An Administrator changes the type of authenticator, e.g., from smart card login to password	X	X

DATA ENTRY AND OUTPUT

Auditable Event	Basic	Medium
Any additional event that is relevant to the security of the CA (such as remote or local data entry or data export); must be documented	X	X

KEY GENERATION

Auditable Event	Basic	Medium
Whenever the CA generates a key (Not mandatory for single session or one-time use symmetric keys)	X	X

PRIVATE KEY LOAD AND STORAGE

Auditable Event	Basic	Medium
The loading of CA, RA, CSS, CMS, or other keys used by the CA in the lifecycle management of certificates	X	X
All access to certificate subject private keys retained within the CA for key recovery purposes	X	X

TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE

Auditable Event	Basic	Medium
Any changes to public keys used by components of the CA to authenticate other components or authorize certificate lifecycle requests (e.g., RA or CMS trust stores)	X	X

PRIVATE AND SECRET KEY EXPORT

Auditable Event	Basic	Medium
The export of private and secret keys (keys used for a single session or message are excluded)	X	X

CERTIFICATE REGISTRATION

Auditable Event	Basic	Medium
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated by a related external system or process	X	X

CERTIFICATE REVOCATION

Auditable Event	Basic	Medium
All records related to certificate revocation request authorization, approval and execution, whether generated directly on the CA or generated by a related external system or process	X	X

CERTIFICATE STATUS CHANGE APPROVAL

Auditable Event	Basic	Medium
All records related to certificate status change request authorization, approval and execution,	X	X

Auditable Event	Basic	Medium
whether generated directly on the CA or generated by a related external system or process		

CA CONFIGURATION

Auditable Event	Basic	Medium
Any security-relevant changes to the configuration of the CA. The specific configuration items relevant to the environment in which the CA operates must be identified and documented.	X	X

ACCOUNT ADMINISTRATION

Auditable Event	Basic	Medium
Roles and users are added or deleted	X	X
The access control privileges of a user account or a role are modified	X	X

CERTIFICATE PROFILE MANAGEMENT

Auditable Event	Basic	Medium
All changes to the certificate profile	X	X

CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT

Auditable Event	Basic	Medium
All changes to the certificate revocation list profile	X	X

MISCELLANEOUS

Auditable Event	Basic	Medium
Appointment of an individual to a designated Trusted Role	X	X

Auditable Event	Basic	Medium
Installation of the Operating System	X	X
Installation of the CA	X	X
Installing hardware cryptographic modules		X
Removing hardware cryptographic modules		X
Destruction of cryptographic modules	X	X
System Startup	X	X
Logon Attempts to CA Applications	X	X
Receipt of Hardware/Software		X
Attempts to set passwords	X	X
Attempts to modify passwords	X	X
Backing up CA internal database	X	X
Restoring CA internal database	X	X
Records of manipulation of critical files (e.g. creation, renaming, moving), critical files will vary between installation, and must be identified in the relevant documentation		X
The date and time any CA artifact is posted to a public repository		X
Access to CA internal database		X
All certificate compromise notification requests	X	X

Auditable Event	Basic	Medium
Loading tokens with certificates		X
Shipment and receipt of tokens containing key material, or tokens that allow access to key material (e.g., HSM operator cards)		X
Zeroizing tokens	X	X
Re-key of the CA	X	X
Configuration changes to the CA server involving: - Hardware	X	X
- Software	X	X
- Operating System	X	X
- Patches	X	X
- Security Profiles		X

PHYSICAL ACCESS / SITE SECURITY

Auditable Event	Basic	Medium
Personnel Access to room housing CA		X
Access to the CA server		X
Known or suspected violations of physical security	X	X

ANOMALIES

Auditable Event	Basic	Medium
Software Error conditions	X	X
Software check integrity failures	X	X
Equipment failure	X	X
Electrical power outages		X

Auditable Event	Basic	Medium
Uninterruptible Power Supply (UPS) failure		X
Network service or access failures that could affect certificate trust		X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X
Resetting Operating System clock	X	X

5.4.2 Frequency of Processing Log

Audit records must be reviewed at least once every month for CAs that issue certificates at Basic or above. CSS, CMS, IDMS and KRS audit log processing frequency shall align with the CA audit log processing frequency.

Auditable Event	Basic	Medium
Assurance Level Review Audit Log	At least once per month	At least once per month

5.4.3 Retention Period for Audit Log

Audit records must be accessible until reviewed, in addition to specific records being archived as described in Section 5.5.

5.4.4 Protection of Audit Log

System configuration and operational procedures must be implemented together to ensure that only authorized individuals may move or archive audit records and that audit records are not modified.

Collection of the audit records from the CA system must be performed by, witnessed by or under the control of trusted roles who are different from the individuals who, in combination, command the CA signature key.

For RA systems, the individual authorized to move or archive records may not hold an RA Trusted Role.

Procedures must be implemented to protect audit records from deletion or destruction before they are reviewed as described in Section 5.4.2. To protect the integrity of audit records, they must be transferred to a backup environment distinct from the environment where the audit records are generated.

5.4.5 Audit Log Backup Procedures

Audit records and audit summaries must be backed up at least monthly.

If audit records are stored locally in the system where the events occur, they must be transferred to a backup environment and protected as described in Section 5.4.4. The backup procedure may be automated or manual, but must occur no less frequently than the audit log review described in Section 5.4.2.

The process for transferring the audit records to the backup environment must be documented.

5.4.6 Audit Collection System (internal vs. external)

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

5.4.7 Notification to Event-causing Subject

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

5.4.8 Vulnerability Assessments

CAs must perform routine vulnerability assessments of the security controls described in the applicable policy.

Automated vulnerability scans, if executed, should be run no less frequently than required by the risk rating of the component.

The methodology, tools and frequency of the vulnerability assessment must be documented.

5.5 RECORDS ARCHIVAL

DigiCert CAs must comply with their respective records retention policies in accordance with whatever laws apply to those entities.

The primary objective of the CA archive is to prove the validity of any certificate (including those revoked or expired) issued by the CA in the event of dispute regarding the use of the certificate.

5.5.1 Types of Records Archived

At a minimum, the following data must be recorded for archive as specified for each assurance level:

Data To Be Archived	Basic	Medium
Certificate Policy	X	X

Data To Be Archived	Basic	Medium
Certification Practice Statement	X	X
Contractual obligations	X	X
Other agreements concerning operations of the CA or KRS	X	X
System and equipment configuration	X	X
Modifications and updates to system or configuration	X	X
All records related to certificate request authorization, approval and signature, whether generated directly on the CA or generated as part of a related external system or process	X	X
All records related to certificate revocation, whether generated directly on the CA or generated as part of a related external system or process	X	X
Subscriber identity Authentication data as per Section 3.2.3	X	X
Documentation of receipt and acceptance of certificates (if applicable)	X	X
Subscriber Agreements	X	X
Documentation of receipt of tokens	X	X
All certificates issued or published	X	X
Record of CA Re-key	X	X

Data To Be Archived	Basic	Medium
Other data or applications to verify archive contents	X	X
Audit summary reports generated by internal reviews and documentation generated during third party audits	X	X
Any changes to the Audit parameters, e.g., audit frequency, type of event audited	X	X
Any attempt to delete or modify the Audit logs	X	X
Whenever the CA generates a key. (Not mandatory for single session or one-time use symmetric keys)	X	X
Changes to trusted public keys used or published by the CA including certificates used for trust between the CA and other components such as CMS, RA, etc	X	X
The export of private and secret keys (keys used for a single session or message are excluded)	X	X
The approval or rejection of a certificate status change request	X	X
Appointment of an individual to a Trusted Role	X	X
Destruction of cryptographic modules	X	X
All certificate compromise notifications	X	X

Data To Be Archived	Basic	Medium
Remedial action taken as a result of violations of physical security	X	X
Violations of Certificate Policy	X	X
Violations of Certification Practice Statement	X	X

5.5.2 Retention Period for Archive

Archive retention periods begin at the key generation event for any CA. For CAs that leverage key-rollover procedures a new retention period begins for each subsequent key generation event.

All archived records are maintained in an accessible fashion for a minimum of 3 years after CA expiration or termination.

RA operations, to include any IT systems that facilitate RA functions, maintains relevant archives for a minimum of 3 years after RA system replacement or termination.

5.5.3 Protection of Archive

Only Auditors, as described in Section 5.2, or other personnel specifically authorized by DigiCert, are permitted to add or delete records from the archive. Deletion of records identified in Section 5.5.1 before the end of the retention period is not permitted under any circumstances. The contents of the archive must not be released except in accordance with Sections 9.3 and 9.4.

Archive media is stored in a safe, secure storage facility geographically separate from the CA in accordance with its records retention policies. The transfer process between the backup environment and archive location are documented.

In order to ensure that records in the archive may be referenced when required, the CA will do one of the following:

- Maintain the hardware or software required to process or read the archive records, or
- Define a process to transfer records to a new format or medium when the old format or medium becomes obsolete and verify the integrity of the records after transfer.

5.5.4 Archive Backup Procedures

On at least an annual basis, DigiCert creates an archive of the data listed in section 5.5.1. Each archive is stored separately and available for integrity verification at a later date. DigiCert stores the archive in a secure location for the duration of the set retention period.

5.5.5 Requirements for Time-stamping of Records

DigiCert automatically time-stamps archived records with system time (non-cryptographic method) as they are created. DigiCert synchronizes its system time at least every eight hours using

a real time value 51 distributed by a recognized UTC(k) laboratory or National Measurement Institute.

5.5.6 Archive Collection System (internal or external)

Archive information is collected internally by DigiCert.

5.5.7 Procedures to Obtain and Verify Archive Information

Details concerning the creation and storage of archive information are found in section 5.5.4. After receiving a request made for a proper purpose by a Customer, its agent, or a party involved in a dispute over a transaction involving the DigiCert PKI, DigiCert may elect to retrieve the information from archival. The integrity of archive information is verified by comparing a hash of the archive disk with the hash originally stored for that disk, as described in Section 5.5.4. DigiCert may elect to transmit the relevant information via a secure electronic method or courier, or it may also refuse to provide the information in its discretion and may require prior payment of all costs associated with the data.

5.6 KEY CHANGEOVER

Each CA's signing key has a validity period as described in Section 6.3.2.

Prior to the end of a CA's signing key validity period, a new CA is established or a re-key on the existing CA must be performed. This is referred to as key changeover. From that time on, only the new key is used to sign CA and Subscriber certificates. The old private key may continue to be used to sign CRLs and OCSP Responder certificates. If the old private key is used to sign OCSP Responder certificates or CRLs that cover certificates signed with that key, the old key must be retained and protected.

After all certificates signed with the old key have expired or been revoked, the CA may issue a final long-term CRL using the old key, with a nextUpdate time past the validity period of all issued certificates. This final CRL is available for all relying parties until the validity period of all issued certificates has passed. Once the last CRL has been issued, the old private signing key of the CA may be destroyed.

When a CA performs a key changeover and thus generates a new public key, the CA notifies all CAs, RAs, and Subscribers that rely on the CA's certificate that it has been changed. The CA does one of the following:

- Generate key rollover certificate, where the new public key is signed by the old private key, and vice versa or
- Obtain a new CA certificate for the new public key from each issuer of the current CA certificate(s).

5.7 COMPROMISE AND DISASTER RECOVERY

DigiCert has an incident handling process, which documents any security incidents. Security incidents may include violation or threat of violation to the system, improper usage, malicious or anomalous activity and violations of the DigiCert FBCA CP, this CPS, and the FBCA CP.

5.7.1 Incident and Compromise Handling Procedures

Digicert notifies the FPKI within 24 hours if the FBCA or an Entity CA experiences the following:

- Suspected or detected compromise of the CA systems;
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components;
- any incident preventing the CA from issuing a CRL prior to the nextUpdate time of the previous CRL;
- suspected or detected compromise of a CSS;
- suspected or detected compromise of an RA.
- The notification must include preliminary remediation analysis.

Once the incident has been resolved, the organization operating the DigiCert provides notification directly to the FPKIPA which includes detailed measures taken to remediate the incident. The notice must include the following:

1. Which CA components were affected by the incident
2. The CA's interpretation of the incident
3. Who is impacted by the incident
4. When the incident was discovered
5. A complete list of all certificates that may have been issued erroneously or are not compliant with the CP/CPS as a result of the incident
6. A statement that the incident has been fully remediated.

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

When computing resources, software, and/or data are corrupted, the CAs DigiCet responds as follows:

- Before returning to operation, ensure that the system's integrity has been restored
- If the CA signature keys are not destroyed, CA operation are reestablished, giving priority to the ability to generate certificate status information within the CRL issuance schedule specified in Section 4.9.7.
- If the CA signature keys are destroyed, CA operation are re-established as quickly as possible, giving priority to the generation of a new CA key pair.

In the event of an incident as described above, DigiCert posts a notice on its web page identifying the incident and provide notification to the FPKIPA. See Section 5.7.1 for contents of the notice.

5.7.3 Entity Private Key Compromise Procedures

5.7.3.1 CA Private Key Compromise Procedures

In the event of a CA private key compromise, the following operations are performed:

- DigiCert immediately informs the FPKIPA and any entities known to be distributing the CA certificate (e.g., in a root store).
- DigiCert requests revocation of any certificates issued to the compromised CA.
- DigiCert generates new keys in accordance with Section 6.1.1.1.

If the CA distributed the public key in a Trusted Certificate, the CA performs the following operations:

- Generate a new Trusted Certificate.
- Securely distribute the new Trusted Certificate as specified in Section 6.1.4.
- Initiate procedures to notify Subscribers of the compromise.

Subscriber certificates issued prior to compromise of the CA private key may be renewed automatically by DigiCert under the new key pair (see Section 4.6) or DigiCert may require Subscribers to repeat the initial certificate application process.

DigiCert will post a notice on its web page describing the compromise. See Section 5.7.1 for contents of the notice.

A DigiCert-appointed governing body is encouraged to also investigate and report to the FPKIPA what caused the compromise or loss.

5.7.3.2 KRS Private Key Compromise Procedures

No stipulation.

5.7.4 Business Continuity Capabilities after a Disaster

DigiCet's repository system isis deployed to provide 24-hour, 365 day per year availability with high levels of repository reliability.

DigiCert has recovery procedures in place to reconstitute the CA within 72 hours of failure.

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

5.8 CA OR RA TERMINATION

For emergency termination, DigiCert follows the notification procedures in Section 5.7.

In the event the decision is made to terminate FBCA operations, of termination of the FBCA operation, the following is accomplished prior to termination:

- Notify all cross-certified Entities.
- Revoke any issued certificates that have not expired
- Generate and publish a final long term CRL with a nextUpdate time past the validity period of all issued certificates. This final CRL must be available for all relying parties until the validity period of all issued certificates has passed.
- Once the last CRL has been issued, destroy the private signing key(s) of the FBCA.
- Transfer all archive data to an archival facility.

Entities will be given as much advance notice as circumstances permit, and attempts to provide alternative sources of interoperation will besought.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

Cryptographic keying material used to sign certificates, CRLs or status information is generated in [FIPS 140] validated cryptographic modules as specified in Section 6.2.1 or modules validated under equivalent international standards. Multiparty control is required for CA key pair generation, as specified in Section 6.2.2.

CA key pair generation creates a verifiable audit trail that the security requirements for procedures were followed. For all levels of assurance, the documentation of the procedure are detailed enough to show that appropriate role separation was used.

For Medium Assurance, an independent third party validates the execution of the key generation procedures either by witnessing the key generation or by examining the signed and documented record of the key generation.

6.1.1.2 Subscriber Key Pair Generation

Subscriber key pair generation may be performed by the subscriber or DigiCert. If DigiCert generates subscriber key pairs, the requirements for key pair delivery specified in Section 6.1.2 must also be met.

Key generation is performed using a FIPS approved method or equivalent international standard.

Either validated software or validated hardware cryptographic modules are used for key generation as specified in Section 6.2.1.

6.1.1.3 CSS Key Pair Generation

Cryptographic keying material used by CSSs to sign status information are generated in [FIPS 140] validated cryptographic modules as specified in Section 6.2.1.

6.1.2 Private Key Delivery to Subscriber

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

For DigiCert, when issuing certificatesthe following requirements apply:

- Where key pairs are generated by the Subscriber or DigiCert, the public key and the Subscriber's identity is delivered securely to DigiCert for certificate issuance.
- The delivery mechanism must bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it is at least as strong as the Subscriber key pair.

6.1.4 CA Public Key Delivery to Relying Parties

Self-signed root CA certificates are conveyed to relying parties in a secure fashion to preclude substitution attacks. Acceptable methods include:

- Secure distribution of the certificate through secure out-of-band mechanisms;
- Download the certificate from a Federal Government operated web site secured with a currently valid certificate and subsequent comparison of the hash of the certificate against a hash value made available via authenticated out-of-band sources (note that hashes posted in-band along with the certificate are not acceptable as an authentication mechanism).

6.1.5 Key Sizes

DigiCert issues certificates according to requirements of the FPKI Common Policy in the following signatures: RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates must contain 2048-, 3072-, or 4096-bit RSA keys, or 256- or 384-bit elliptic curve keys.

6.1.5 Key Sizes

DigiCert issues certificates according to requirements of the FPKI Common Policy in the following signatures: RSA PKCS #1, RSASSA-PSS, or ECDSA signatures; additional restrictions on key sizes and hash algorithms are detailed below. Certificates must contain 2048-, 3072-, or 4096-bit RSA keys, or 256- or 384-bit elliptic curve keys.

	CA Certificates that expire on or before December 31, 2030	CA Certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

	Subscriber certificates that expire on or before December 31, 2030	Subscriber certificates that expire after December 31, 2030
Minimum Key Size	RSA: 2048 Elliptic Curve: 256	RSA: 3072 Elliptic Curve: 256
Hash Algorithm	SHA-256, SHA-384, or SHA-512	SHA-256, SHA-384, or SHA-512

Use of Transport Layer Security (TLS) or another protocol providing similar security to accomplish any of the requirements of the FBCA CP and this CP requires at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 2048-bit RSA or equivalent for the asymmetric keys. After December 31, 2030, use of TLS or another protocol providing similar security to accomplish any of the requirements of this CP requires at a minimum AES (128 bits) or equivalent for the symmetric key, and at least 3072-bit RSA or equivalent for the asymmetric keys.

6.1.6 Public Key Parameters Generation and Quality Checking

Public key parameters generation and quality checking is conducted in accordance with [NIST SP 800-89]. Key validity must be confirmed in accordance with [NIST SP 800-56A].

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

Public keys that are bound into certificates are certified for use in signing or encrypting, but not both, except as specified below. The use of a specific key is determined by the key usage extension in the X.509 certificate.

All certificates includes a critical Key Usage extension * Certificates to be used for authentication must set only the digitalSignature bit. * Certificates to be used by Human Subscribers only for digital signatures must set the digitalSignature and nonRepudiation bits. * Certificates that have the nonRepudiation bit set, must not have keyEncipherment bit or keyAgreement bit set. * Certificates to be used for encryption (RSA) must set the keyEncipherment bit. * Certificates to be used for key agreement (ECC) must set the keyAgreement bit. * CA certificates must set only cRLSign and keyCertSign bits. Keys associated with CA certificates must be used only for signing certificates and CRLs.

Keys associated with Device Subscriber certificates may be used for digital signature (including authentication), encryption, or both. Except for OCSP Responder certificates, device certificates must not assert the nonRepudiation bit.

Certificates may include a single key for use with encryption and signature in support of legacy applications. Such dual-use certificates must be generated and managed in accordance with their respective signature certificate requirements, except where otherwise noted in the FBCA CP and this CPS. Such dual-use certificates never assert the non-repudiation key usage bit, and are not used for authenticating data that will be verified on the basis of the dual-use certificate at a future time. Entities are encouraged at all levels of assurance to issue Subscribers two key pairs, one for key management and one for digital signature and authentication.

For all Subscriber certificates issued after June 30, 2019, the Extended Key Usage extension are always present. Extended Key Usage OIDs are consistent with key usage bits asserted. The Extended Key Usage extension does not contain anyExtendedKeyUsage {2.5.29.37.0}.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is [FIPS 140], Security Requirements for Cryptographic Modules. A FIPS 140 Level 1 or higher validated cryptographic module is used for all cryptographic operations. Cryptographic modules are minimally validated to the FIPS 140 level identified in this section. The table below summarizes the minimum FIPS 140 requirements for cryptographic modules; higher levels may be used.

Assurance Level	CA (DigiCert)	CMS & CSS	Subscriber	RA (DigiCert)
Basic	Level 2	Level 2	Level 1	Level 1
Medium	Level 3 (Hardware)	Level 2 (Hardware)	Level 1	Level 2 (Hardware)
Medium Hardware	Level 3 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)	Level 2 (Hardware)

Any pseudo-random numbers used for key generation material must be generated using a FIPS-validated cryptographic module.

6.2.1.1 Custodial Subscriber Key Stores

Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location. When a collection of private keys for Subscriber certificates are held in a single location, there is a higher risk associated with compromise of that cryptographic module than that of a single Subscriber.

Cryptographic modules for Custodial Subscriber Key Stores must be no less than FIPS 140 Level 2 Hardware.

In addition, authentication to the Cryptographic Device in order to activate the private key associated with a given certificate requires authentication commensurate with the assurance level of the certificate.

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

Use of the DigiCert CA private signing key and CSA private signing key requires action by multiple persons at Medium Assurance as set forth in Section 5.2.2 of this CPS.

6.2.3 Private Key Escrow

CA private keys are never escrowed.

Human Subscriber key management keys are not escrowed.

Subscriber private signature keys must not be escrowed.

Subscriber private dual use keys must not be escrowed. If a device has a separate key management key certificate, the key management private key is not escrowed.

6.2.4 Private Key Backup

All backups of CA and CSS private signature keys are accounted for and protected under the same multi-person control as the original signature key. At least one copy of the CA private signature key are stored off site.

For all other keys, backup, when permitted, provides security controls consistent with the protection provided by the original cryptographic module. Backed up private signature key(s) are not exported or stored in plaintext form outside the cryptographic module.

Private Key Backup	Policies	Requirement
CA	all applicable policies	Required
CSS	all applicable policies	Optional
Hardware Subscriber Key Management	id-fpki-certpcy-mediumHardware id-fpki-certpcy-mediumHW-CBP	Optional
Hardware Device	id-fpki-certpcy-mediumDeviceHardware	Optional
Software Signature and Authentication	id-fpki-certpcy-basicAssurance id-fpki-certpcy-mediumAssurance id-fpki-certpcy-medium-CBP	Optional
Software Subscriber Key Management	id-fpki-certpcy-basicAssurance id-fpki-certpcy-mediumAssurance id-fpki-certpcy-medium-CBP	Optional
Software Device	id-fpki-certpcy-mediumDevice	Optional

6.2.5 Private Key Archival

CA private signature keys and Subscriber private signature keys are not archived.

DigiCert does not maintain an archive of escrowed Subscriber private key management keys.

6.2.6 Private Key Transfer into or from a Cryptographic Module

A CA private key does not exist in plain text outside the cryptographic module.

CA and CSS C private signature keys may be exported from the cryptographic module only to perform CA key backup procedures as described in Section 6.2.4.

If any private key is transported from one cryptographic module to another, the private key is protected using a FIPS approved algorithm and at a bit strength commensurate with the key being transported. Private keys never exist in plaintext form outside the cryptographic module boundary.

Private or symmetric keys used to encrypt other private keys for transport are protected from disclosure.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation beyond that specified in [FIPS-140].

6.2.8 Method of Activating Private Key

Cryptographic modules must be protected from unauthorized access.

Subscriber private key activation requirements are detailed in the following table:

Policy Asserted	Activation Requirements
id-fpki-certpcy-basicAssurance id-fpki-certpcy-mediumAssurance id-fpki-certpcy-medium-CBP	Passphrases, PINs, or biometrics. When passphrases or PINs are used, they must be a minimum of six (6) characters. Entry of activation data must be protected from disclosure (i.e., the data should not be displayed while it is entered).

6.2.9 Method of Deactivating Private Key

DigiCert's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. DigiCert never leaves its HSM devices in an active unlocked or unattended state. Subscribers should deactivate their Private Keys via logout and removal procedures when not in use. CA Hardware cryptographic modules must be physically secured per requirements in Section 5.1 when not in use.

6.2.10 Method of Destroying Private Key

Individuals in trusted roles will destroy all copies of CA, RA, and CSS private signature keys and activation data (e.g., operator card set or tokens) when they are no longer needed.

Subscribers either surrender their cryptographic modules to DigiCert personnel for destruction or destroy their private signature keys when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

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

Public key archival is in accordance with Section 5.5.

6.3.2 Certificate Operational Periods and Key Pair Usage Periods

A CA private key may be used to sign CRLs and OCSP responder certificates for the entire usage period. All certificates signed by a specific CA key pair must expire before the end of that key pair's usage period.

Key	Private Key Validity	Certificate Validity
Root CA certificate (self-signed)	20 years	20 years
Federal Bridge CA certificate	10 years	10 years
Intermediate/Signing CA certificate	10 years	10 years
Cross Certificate	3 years	3 years
Subscriber Authentication	3 years	3 years
Subscriber Signature	3 years	3 years
Subscriber Encryption	Unrestricted	3 years
OCSP Responder	3 years	120 days
Device	3 years	3 years

The validity period of the subscriber certificate must not exceed the routine re-key Identity Requirements as specified in Section 3.3.1.

6.4 ACTIVATION DATA

6.4.1 Activation Data Generation and Installation

The activation data used to unlock CA or subscriber private keys, in conjunction with any other access control, has an appropriate level of strength for the keys or data to be protected. If the activation data is transmitted, it is via an appropriately protected channel, and distinct in time and place from the associated cryptographic module. Where the CA uses passwords as activation data for the CA signing key, at a minimum the activation data must be changed upon CA re-key.

For Medium AssuranceRA and Subscriber activation data may be user-selected. The strength of the activation data meets or exceeds the requirements for authentication mechanisms stipulated for

Level 2 in [FIPS 140]. If the activation data is transmitted, it is via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

6.4.2 Activation Data Protection

Data used to unlock private keys is protected from disclosure by a combination of cryptographic and physical access control mechanisms. Activation data must be:

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

The protection mechanism includes a facility to temporarily lock the account, or terminate the application, after a predetermined number of failed login attempts as set forth in the DigiCert FBCA CP and this CPS.

6.4.3 Other Aspects of Activation Data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

For CAs, and DDSs the computer security functions listed below are required. These functions may be provided by the operating system, or through a combination of operating system, software, and physical safeguards. The CA and its ancillary parts includes the following functionality (these functions pertain to all system software layers, where applicable):

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes;
- Require use of cryptography for session communication and database security;
- Require self-test security-related CA services;
- Require a trusted path for identification of all users;
- Provide residual information protection; and
- Require recovery from key or system failure.

For Certificate Status Servers, the computer security functions listed below are required (these functions pertain to all system software layers, where applicable):

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Enforce domain integrity boundaries for security critical processes;
- Provide residual information protection; and
- Require recovery from key or system failure.

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

- Authenticate the identity of users before permitting access to the system or applications;
- Manage privileges of users to limit users to their assigned roles;
- Generate and archive audit records for all transactions; (see Section 5.4)
- Enforce domain integrity boundaries for security critical processes;
- Provide residual information protection; and
- Require recovery from system failure.

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

6.5.2 Computer Security Rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System Development Controls

The System Development Controls for CAs (including any remote workstations used to administer the CA) and RAs at the Basic Assurance level and above are as follows:

- Where open source software has been utilized, the applicant demonstrates that security requirements were achieved through software verification and validation and structured development/life-cycle management.
- Hardware and software used to administer or operate the CA is procured and shipped in a fashion to reduce the likelihood that any particular component was tampered with (e.g., by ensuring the equipment was randomly selected at time of purchase).
- Custom hardware and software is developed in a controlled environment, and the development process is defined and documented. This requirement does not apply to commercial off-the-shelf hardware or software.

- The CA hardware and software, including all system software layers, is dedicated to operating and supporting the CA (i.e., the systems and services dedicated to the issuance and management of certificates). There is no other applications, hardware devices, network connections, or component software installed which are not part of the CA operation, administration, monitoring and security compliance of the system. CA hardware and system software layers may support multiple CAs and their supporting systems, provided all systems have comparable security controls and are dedicated to the support of the CA in compliance of this CP.
- Proper care is taken to prevent malicious software from being loaded onto the CA equipment. All applications required to perform the operation of the CA is obtained from documented sources. Except for Offline CAs, CA and RA hardware and software must be scanned for malicious code on first use and periodically thereafter.
- Hardware and software updates are purchased or developed in the same manner as original equipment, and be installed by trusted and trained personnel in a defined manner.

6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades is documented and controlled. There is a mechanism for detecting unauthorized modification to CA software or configuration. The CA software, when first loaded, is verified as being that supplied from the vendor, with no modifications, and be the version intended for use. DigiCert periodically verifies the integrity of the software.

For offline CAs (e.g., the FBCA), the integrity of the software is verified when the CA is powered on.

6.6.3 Life Cycle Security Controls

No stipulation.

6.7 NETWORK SECURITY CONTROLS

This section does not apply to offline CAs.

A network guard, firewall, or filtering router protects network access to CA. The network guard, firewall, or filtering router limits services allowed to and from the CA equipment to those required to perform CA and KRS functions.

Protection of CA equipment is provided against known network attacks. All unused network ports and services are turned off. Any network software present on the CA equipment is necessary to the functioning of the CA application.

Any boundary control devices used to protect the local area network on which PKI equipment is hosted denies all but the necessary services to the PKI equipment.

RAs, repositories, CSSs, and remote workstations used to administer the CAs employs appropriate network security controls. Networking equipment turns off unused network ports and services. Any network software present is necessary to the function of the equipment.

Any remote workstation used to administer the CA uses a Virtual Private Network (VPN) to access the CA. The VPN must be configured for mutual authentication, encryption, and integrity. If mutual authentication is shared secret based, the shared secret is changed at least annually, must be randomly generated, and must have entropy commensurate with the cryptographic strength of certificates issued by the PKI being administered.

The CA permits remote administration only after successful multi-factor authentication of the Trusted Role at a level of assurance commensurate with that of the CA.

6.8 TIME-STAMPING

Asserted times must be accurate to within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1 of the FBCA CP and this CPS.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

All other certificates are compatible with X.509 Certificate and CRL Extensions Profile [FPKI-Prof].

7.1.1 Version Number(s)

Certificates are of type X.509 v3 (populate version field with integer "2").

7.1.2 Certificate Extensions

For all CAs, use of standard certificate extensions must comply with [RFC 5280].

CA certificates does not include critical private extensions.

When used in Subscriber certificates, critical private extensions are interoperable in their intended community of use.

DigiCert and Subscriber certificates may include any extensions as specified by [RFC 5280] in a certificate, but includes those extensions required by the FBCA CP and this CPS. Any optional or additional extensions does not conflict with the applicable certificate and CRL profiles identified in Section 7.1

7.1.3 Algorithm Object Identifiers

Certificates issued by DigiCert identifies the signature algorithm using one of the following OIDs:

Signature Algorithm	Description	Object Identifier (OID)
sha256WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11 }	1.2.840.113549.1.1.11

Signature Algorithm	Description	Object Identifier (OID)
sha384WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12 }	1.2.840.113549.1.1.12
sha512WithRSAEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 13 }	1.2.840.113549.1.1.13
id-RSASSA-PSS	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10 }	1.2.840.113549.1.1.10
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }	1.2.840.10045.4.3.2
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }	1.2.840.10045.4.3.3
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 4 }	1.2.840.10045.4.3.4
ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 1 }	1.2.840.10045.4.3.1
ecdsa-with-SHA256	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 2 }	1.2.840.10045.4.3.2
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2(3) 3 }	1.2.840.10045.4.3.3
ecdsa-with-SHA5128	{ iso(1) member-body(2) us(840) ansi-X9-62(10045)	1.2.840.10045.4.3.4

Signature Algorithm	Description	Object Identifier (OID)
	signatures(4) ecdsa-with-SHA2(3) 4 }	

The PSS padding scheme OID is independent of the hash algorithm. The hash algorithm is specified as a parameter (for details, see [PKCS#1]). Certificates must use the SHA-256 hash algorithm when generating RSASSA-PSS signatures. The following OID must be used to specify the hash in an RSASSA-PSS digital signature:

Signature Algorithm	Description	Object Identifier (OID)
id-sha256	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1 }	2.16.840.1.101.3.4.2.1
id-sha512	{ joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 3 }	2.16.840.1.101.3.4.2.3

Certificates must use the following OIDs to identify the algorithm associated with the subject key:

Public Key Algorithm	Description	Object Identifier (OID)
rsaEncryption	{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }	1.2.840.113549.1.1.1
id-ecPublicKey	{ iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1 }	1.2.840.10045.2.1

7.1.4 Name Forms

Where required as set forth in Section 3.1.1, the subject and issuer fields of the base certificate are populated with an X.500 Distinguished Name. Distinguished names are composed of standard attribute types, such as those identified in [RFC 5280].

7.1.5 Name Constraints

DigiCert may include name constraints in the nameConstraints field when appropriate. For publicly-trusted TLS certificates, DigiCert will follow the requirements of section 7.1.5 of the Baseline Requirements and as the following sections specify.

7.1.6 Certificate Policy Object Identifier

All certificates issued by the FBCA includesa certificate policies extension asserting one or more of the certificate policy OID(s) appropriate to the level of assurance with which it was issued. See Section 1.2 for specific OIDs in the FBCA CP and this CPS.

DigiCert does not assert the FBCA CP OIDs in any certificates it issues, except in the policyMappings extension establishing an equivalency between an FBCA OID and an OID in this CPS.

DigiCert certificates assert at least one certificate policy OID as specified in Section 1.2 of this CPS in the certificate policies extension.

Delegated OCSP Responder certificates asserts all policy OIDs for which they are authoritative.

7.1.7 Usage of Policy Constraints Extension

For Subordinate CA certificates inhibitPolicyMapping, skip certs must be set to 0. For cross-certificates inhibitPolicyMapping, skip certs must be set appropriately. When requireExplicitPolicy is included skip certs must be set to 0.

7.1.8 Policy Qualifiers Syntax and Semantics

Certificates issued by DigiCert may contain policy qualifiers identified in [RFC 5280].

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

Certificates contain a non-critical certificate policies extension.

7.2 CRL PROFILE

If a reasonCode CRL entry extension is present, the CRLReason must indicate the most appropriate reason for revocation of the certificate unless the reason is unspecified. DigiCert specifies the following reason codes from RFC 5280, section 5.3.1 as appropriate for most instances when used in accordance with the practices in this section and this CPS:

- unspecified (0)
- keyCompromise (1)
- cACompromise (2)
- affiliationChanged (3)
- superseded (4)
- cessationOfOperation (5)

7.2.1 Version number(s)

CAs issue X.509 version two (2) CRLs.

7.2.2 CRL and CRL Entry Extensions

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Subject Key Identifier of the CRL issuer certificate
Invalidity Date	Optional date in UTC format
Reason Code	Specify reason for revocation in list of reason codes in section 7.2, if included.

7.3 OCSP PROFILE

If implemented, Certificate Status Servers (CSS) sign responses using algorithms designated for CRL signing.

All CSSs accept and return SHA-1 hashes in the CertID and responderID fields. CSS may accept and return additional hash algorithms within the CertID fields. CSSs does not return any response containing a hash algorithm in the CertID that differs from the CertID in the request.

7.3.1 Version Number(s)

CSSs must use OCSP version 1.

7.3.2 OCSP Extensions

No stipulation.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

DigiCert is subject to an annual review by the FPKIPA to ensure their policies and operations remain consistent with the policy mappings in the certificate issued to DigiCert by the FBCA.

DigiCert has a compliance audit mechanism in place to ensure that the requirements of the DigiCert FBCACP and this CPS are being implemented and enforced. The DCPA is responsible for ensuring annual audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

DigiCert is subject to an annual audit. The audit includes all CAs, as well as CSS, CMS & RAs, and supporting repositories. Where a status server is specified in certificates issued by DigiCert, the status server is subject to the same compliance audit requirements as the corresponding CA. For example, if an OCSP server is specified in the authority information access extension in certificates issued by a CA, that server isreviewed as part of DigiCert's compliance audit.

The compliance audit is carried out in accordance with the requirements as specified in the FPKI Annual Review Requirements document.

The DCPA has the right to require periodic and aperiodic compliance audits or inspections of subordinate CA or RA operations to validate that the subordinate entities are operating in accordance with the security practices and procedures described in the DigiCert FBCA CPS.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The auditor demonstrates competence in the field of compliance audits. At the time of the audit, the CA compliance auditor is thoroughly familiar with the requirements for issuance and management of their certificates. The compliance auditor performs such compliance audits as a regular ongoing business activity.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The compliance auditor either is a private firm, that is independent from the entity being audited, or it is sufficiently organizationally separated from that entity to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To ensure independence and objectivity, the compliance auditor may not have served the entity in developing or maintaining DigiCert's CA Facility or the DigiCert FBCA CPS.

8.4 TOPICS COVERED BY ASSESSMENT

The purpose of a compliance audit of a PKI must be to verify that it is operating in accordance with this CPS that meets the requirements of the DigiCert FBCA CP, as well as any MOAs between DigiCert. Components other than CAs may be audited fully or by using a representative sample.

If the auditor uses statistical sampling, all PKI components, PKI component managers and operators are considered in the sample. The samples must vary on an annual basis.

A full compliance audit for the PKI covers all aspects within the scope identified above.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

When the DigiCert compliance auditor finds a discrepancy between how DigiCert is designed or is being operated or maintained, and the requirements of the DigiCert FBCA CP, any applicable MOAs, or this CPS, the following actions must be performed:

- The compliance auditor documents the discrepancy;
- The compliance auditor notifies the responsible party promptly;
- DigiCert determines what further notifications or actions are necessary to meet the requirements of the DigiCert FBCA CP, this CPS, and any relevant MOA provisions. DigiCert must proceed to make such notifications and take such actions without delay.

When the FPKIPA receives a report of audit deficiency from DigiCert, the FPKIPA may direct the FPKIMA to take additional actions to protect the level of trust in the infrastructure.

8.6 COMMUNICATION OF RESULTS

On an annual basis, the DCPA submits an annual review package to the FPKIPA. This package must be prepared in accordance with the FPKI Annual Review Requirements document and includes an assertion from a voting member of the DCPA that all PKI components have been audited - including any components that may be separately managed and operated. The package identifies the versions of the DigiCert FBCA CP and this CPS used in the assessment. Additionally, where necessary, the results are communicated as set forth in Section 8.5 above.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 FEES

9.1.1 Certificate Issuance or Renewal Fees

DigiCert may charge fees for certificate issuance and renewal.

9.1.2 Certificate Access Fees

Section 2 of this CP requires that CA certificates be publicly available. DigiCert may charge fees for access to their databases of Subscriber Certificates.

9.1.3 Revocation or Status Information Access Fees

DigiCert does not charge additional fees for revoking certificates or access to CRLs and OCSP status information.

9.1.4 Fees for Other Services

DigiCert shall not charge a fee for access to the DigiCert FBCA CP or this CPS. Any use made for purposes other than simply viewing the document, such as reproduction, redistribution, modification, or creation of derivative works, shall be subject to a license agreement with the entity holding the copyright to the document.

9.1.5 Refund Policy

No stipulation.

9.2 FINANCIAL RESPONSIBILITY

Entities acting as Relying Parties determines what financial limits, if any, they wish to impose for certificates used to complete a transaction.

9.2.1 Insurance Coverage

DigiCert 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

CA information identified in Section 2 not requiring protection is made publicly available. Public access to organizational information must be determined by the respective organization.

9.3.1 Scope of Confidential Information

The following information is considered confidential and protected against disclosure using a reasonable degree of care:

- Private Keys;
- Activation data used to access Private Keys or to gain access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability ofinformation;
- Information held by DigiCert as private information in accordance with Section9.4;
- Audit logs and archive records; and
- Transaction records, financial audit records, and external or internal audit trail records and any audit reports (with the exception of an auditor's letter confirming the effectiveness of the controls set forth in this CPS).

9.3.2 Information Not Within the Scope of Confidential Information

DigiCert may treat any information not listed as confidential in the DigiCert FBCA CPS as public information.

9.3.3 Responsibility to Protect Confidential Information

DigiCert shall contractually obligate employees, agents, and contractors to protect confidential information. DigiCert shall provide training to employees on how to handle confidential information. DigiCert is responsible for maintaining the confidentiality of shared information clearly marked or labeled as confidential. DigiCert treats such information with the same degree of care and security as it treats its own confidential information.

9.4 PRIVACY OF PERSONAL INFORMATION

9.4.1 Privacy Plan

DigiCert shall create and follow a publicly posted privacy policy that specifies how it handles personal information.

9.4.2 Information Treated as Private

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

For DigiCert, collection of PII must be limited to the minimum necessary to validate the identity of the subscriber. This may include attributes that corelate identity evidence to authoritative sources. DigiCert must provide explicit notice to the subscriber regarding the purpose for collecting and maintaining a record of the PII necessary for identity proofing and the consequences for not providing the information. PII collected for identity proofing purposes must not be used for any other purpose.

9.4.3 Information Not Deemed Private

Subject to local laws, private information does not include Certificates, CRLs, or their contents.

Information included in certificates is not subject to protections outlined in Section 9.4.2, but may not be sold to a third party.

9.4.4 Responsibility to Protect Private Information

Sensitive information is stored securely and may be released only in accordance with other stipulations in Section 9.4.

All information collected as part of the identity proofing process is protected to ensure confidentiality and integrity. In the event DigiCert terminates PKI activities, it is responsible for disposing of or destroying sensitive information, including PII, in a secure manner, and maintaining its protection from unauthorized access until destruction.

9.4.5 Notice and Consent to Use Private Information

Subscribers consent to the global transfer and publication of any personal data contained in Certificates.

9.4.6 Disclosure Pursuant to Judicial or Administrative Process

DigiCert 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

DigiCert does not knowingly violate intellectual property rights held by others.

9.5.1 Property Rights in Certificates and Revocation Information

DigiCert retains all intellectual property rights in and to the Certificates and revocation information that they issue. DigiCert and customers shall grant permission to reproduce and distribute Certificates on a nonexclusive royalty-free basis, provided that they are reproduced in full and that use of Certificates is subject to the Relying Party Agreement referenced in the Certificate. DigiCert, Affiliates, and customers shall grant permission to use revocation information to perform Relying Party functions subject to the applicable CRL usage agreement, Relying Party Agreement, or any other applicable agreements.

9.5.2 Property Rights in the CP

DigiCert retains all intellectual property rights in and to the DigiCert FBCA CP.

9.5.3 Property Rights in Names

Subscribers and Applicants retain all rights it has (if any) in any trademark, service mark, or trade name contained in any Certificate and distinguished name within any Certificate issued to such Subscriber or Applicant.

9.5.4 Property Rights in Keys and Key Material

Key Pairs corresponding to Certificates of CAs and end-user Subscribers are the property of DigiCert and end-user Subscribers that are the respective subjects of the Certificates, regardless of the physical medium within which they are stored and protected, and such persons retain all intellectual property rights in and to these key pairs.

9.5.5 Violation of Property Rights

DigiCert shall not knowingly violate the intellectual property rights of any third party

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

DigiCert represents to Subscribers and Relying Parties that they comply, in all material aspects, with the DigiCert FBCA CP and this CPS. Subscriber Agreements may include additional representations and warranties that do not contradict or supersede this CP.

9.6.2 RA Representations and Warranties

At a minimum, DigiCert RA agents represent that they have followed the DigiCert FBCA CP and this CPS when participating in the issuance and management of Certificates. Subscriber Agreements may include additional representations and warranties.

9.6.3 Subscriber Representations and Warranties

For Medium Assurance levels, a Subscriber is required to sign a document containing the requirements the Subscriber meets respecting protection of the private key and use of the certificate before being issued the certificate. For Basic Assurance level, the Subscriber is required to acknowledge his or her obligations respecting protection of the private key and use of the certificate before being issued the certificate.

Subscribers of DigiCert at Basic and Medium Assurance Levels must agree to the following:

- Accurately represent themselves in all communications with the PKI authorities.
- Protect their private keys at all times, in accordance with the FBCA CP, the DigiCert FBCA CP, as stipulated in their certificate acceptance agreements, and local procedures.
- Promptly notify DigiCert upon suspicion of loss or compromise of their private keys. Such notification must be made directly or indirectly through mechanisms consistent with the DigiCert FBCA CPS.
- Abide by all the terms, conditions, and restrictions levied on the use of their private keys and certificates.

9.6.4 Relying Party Representations and Warranties

Relying Parties follows the procedures and make the representations required by the DigiCert FBCA CPS and in the applicable Relying Party Agreement prior to relying on or using a Certificate.

Relying Party Agreements may include additional representations and warranties.

9.6.5 Representations and Warranties of Other Participants

Affiliated Organizations authorizes the affiliation of subscribers with the organization, and must inform DigiCert of any severance of affiliation with any current subscriber.

9.7 DISCLAIMERS OF WARRANTIES

Except as expressly stated otherwise herein, an applicable extended warranty protection plan or as limited by law, DigiCert disclaims all warranties and obligations related to this CPS.

9.8 LIMITATIONS OF LIABILITY

DigiCert may limit their liability to any extent not otherwise prohibited by this CPS, provided that DigiCert remains responsible for complying with this CP and the DigiCert FBCA CPS.

To the extent DigiCert has issued and managed the Certificate(s) at issue in compliance with this CP and its CPS, DigiCert shall have no liability to the Subscriber, any Relying Party, or any other third parties for any damages or losses suffered as a result of the use or reliance on such Certificate(s). To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall limit DigiCert's and the applicable Affiliates' liability outside the context of any extended warranty protection program. Limitations of liability shall include an exclusion of indirect, special, incidental, and consequential damages.

The liability (and/or limitation thereof) of Subscribers shall be as set forth in the applicable Subscriber Agreements.

The liability (and/or limitation thereof) of Relying Parties shall be as set forth in the applicable Relying Party Agreements.

9.9 INDEMNITIES

9.9.1 Indemnification by an Issuer CA

No Stipulation.

9.9.2 Indemnification by Subscribers

DigiCert shall include any indemnification requirements for Subscribers in the DigiCert FBCA CPS and in their Subscriber Agreements.

To the extent permitted by applicable law, Subscribers are required to indemnify DigiCert for:

- Falsehood or misrepresentation of fact by the Subscriber on the Subscriber's Certificate Application,
- Failure by the Subscriber to disclose a material fact on the Certificate Application, if the misrepresentation or omission was made negligently or with intent to deceive any party,
- The Subscriber's failure to protect the Subscriber's Private Key, to use a trustworthy system, or to otherwise take the precautions necessary to prevent the compromise, loss, disclosure, modification, or unauthorized use of the Subscriber's private key, or
- The Subscriber's use of a name (including without limitation within a common name, domain name, or e-mail address) that infringes upon the intellectual property rights of a third party. The applicable Subscriber Agreement may include additional indemnity obligations.

9.9.3 Indemnification by Relying Parties

DigiCert shall include any indemnification requirements for Relying Parties in the DigiCert FBCA CPS.

9.10 TERM AND TERMINATION

9.10.1 Term

This CPS 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 CPS as amended from time to time, shall 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 CPS' 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

For DigiCert, any planned change to the infrastructure that has the potential to affect the FPKI operational environment must be communicated to the FPKIPA at least two weeks prior to implementation. All new artifacts (CA certificates, CRL DP, AIA and/or SIA URLs, etc.) produced as a result of the change must be provided to the FPKIPA within 24 hours following implementation.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

Amendments are made by posting an updated version of the CPS to the online repository upon review and approval by the DCPA while working with the FPKIPA. Updates supersede any designated or conflicting provisions of the referenced version of the CPS. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA working with the FPKIPA. The DCPA reviews this CP annually.

9.12.2 Notification Mechanism and Period

DigiCert will post notice on its website of any proposed significant revisions to this CPS. Although DigiCert may include a final date for receipt of comments and the proposed effective date, DigiCert is not required to have a fixed notice-and-comment period. DigiCert and the DCPA reserve the right to amend the CPS without notification for amendments that are not material, including without limitation corrections of typographical errors, changes to URLs, and changes to contact information. The DCPA's decision to designate amendments as material or non- material shall be within the DCPA's sole discretion.

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 CPS will also contain a revised OID. Otherwise, amendments do not require an OID change.

9.13 DISPUTE RESOLUTION PROVISIONS

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall contain a dispute resolution clause. Unless otherwise approved by DigiCert, the procedure to resolve disputes involving DigiCert require an initial negotiation period of sixty (60) days followed by litigation in the federal or state court encompassing Salt Lake County, Utah, in the case of claimants who are U.S. residents, or, in the case of all other claimants, arbitration administered by the International Chamber of Commerce ("ICC") in accordance with the ICC Rules of Conciliation and Arbitration.

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 CPS and all proceedings related hereunder, including tort claims, without regard to any conflicts of law principles, and Salt Lake County, Utah shall be the non-exclusive venue and shall have jurisdiction over such proceedings.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, each Issuer CA shall (i) be licensed in each jurisdiction where it operates where licensing is required by the law of such jurisdiction for the issuance of Certificates, and (ii) meet the requirements of European data protection laws and shall establish and maintain appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

DigiCert shall contractually obligate parties using products and services issued under this CPS, such as Subscribers and Relying Parties, to the relevant provisions herein. This CPS does not give any third-party rights under such agreements.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement (attorneys' fees and waiver of rights)

DigiCert may seek indemnification and attorneys' fees from a party for damages, losses, and expenses related to that party's conduct. DigiCert's failure to enforce a provision of this CPS does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this CPS. 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 CPS 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.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting DigiCert.

9.17 OTHER PROVISIONS

No stipulation.