Version 5.12
October 31, 2022
2801 N.
Thanksgiving Way
Suite 500
Lehi, UT 84043
USA
Tel: 1-801-877-2100
Fax: 1-801-705-0481

1-April-2015	Made additional changes based on FPKI CPWG review.	4.08
7-October-2014	Updated for consistency with FBCA CP v. 2.27	4.07
14-May-2014	Updated to comply with changes to Baseline Requirements and the EV Guidelines.	4.06
2-May-2013	Updated mailing address, removed references to Adobe CDS Program, revised explanation of Level 2 identification requirements, revised private key management provisions and key ceremony witness requirements.	4.05
10-May-2012	Updated to include provisions set forth in the Baseline Requirements, to add EV Code Signing, improve readability, and to modify requirements related to IGTF Certificates.	4.04
3-May-2011	Policy OIDs revised for certain certificate types and minor updates made to various sections.	4.03
29-October-2010	Changes made in response to comments from the FPKI CPWG regarding certificate status services, trusted roles, and off-site backup of archive.	4.02
26-August-2010	Updated the process used to authenticate the certificate requester's authority under section 3.2.5 for code signing certificates issued to organizations	4.01
2-August-2010	This version 4.0 replaces the DigiCert Certificate Policy and Certification Practices Statement, Version 3.08, dated May 29, 2009.	4.0

The OID arc for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114] TJA41)

Practices Statement (RPS) under which the RA operates.

An Issuer CA that relies on a variety of RAs or IdMs to support various communities of interest may submit an RPS for each RA or IdM to the DCPA for approval. The RPS must contain details necessary for the DCPA to determine how the RA achieves compliance with this Policy.

Necessary details include how the RA's process or IdM establishes the identities of applicants, how the integrity and authenticity of such identifying information is securely maintained and managed, and how changes and updates to such information are communicated to the Issuer CA.

Subscribers use DigiCert's services and PKI to support transactions and communications. Subscribers under this CP include all end users (including entities) of certificates issued by an Issuer CA. A subscriber is the entity named as the end-user Subscriber of a certificate. End-user Subscribers may be individuals, organizations or, infrastructure components such as firewalls, routers, trusted servers or other devices used to secure communications within an Organization.

Subscribers are not always the party identified in a Certificate, such as when Certificates are issued to an organization's employees. The *Subject* of a Certificate is the party named in the

Certificate. A *Subscriber*, as used herein, refers to both the subject of the Certificate and the entity that contracted with the Issuer CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an *Applicant*.

CAs are technically also subscribers of certificates within the DigiCert Public PKI, either as the primary Certificate Authority issuing a self- signed Certificate to itself, or as an Issuer CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CP, however, apply only to end- user Subscribers.

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by the Issuer CA. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. A Relying party may also be a Subscriber of the DigiCert Public PKI hierarchy.

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

CERTIFICATE USAGE

A *digital Certificate* (or *Certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

A *time-stamp token* (*TST*) cryptographically binds a representation of data to a particular time stamp, thus establishing evidence that the data existed at a certain point in time.

Individual Certificates are normally used by individuals to sign and encrypt e-mail and to authenticate to applications (client authentication). While an individual certificate may be used for other purposes, provided that a Relying Party is able to reasonably rely on that certificate and the usage is not otherwise prohibited by law, by this CP, by any CPS under which the certificate has been issued and any agreements with Subscribers.

Organizational Certificates are issued to organizations after authentication that the

NAMING

Issuer CAs shall issue Certificates with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards. Level 1 Certificates may include a null subject DN if they include at least one alternative name form that is marked critical. Subject Alternate Name forms may be included in Certificates if they are marked non-critical. Other attributes may be present within the subject field. If present, other attributes must contain information that has been verified by the CA or RA.

When applicable, Issuer CAs shall use distinguished names to identify both the entity (i.e. person, organization,

The names of Subscribers shall be unique within a subordinate Issuer CA's and Customer's Sub-domain for a specific type of Certificate. Name uniqueness is not violated when multiple certificates are issued to the same entity.

For publicly-trusted OV/DV TLS/SSL and EV TLS/SSL Certificates, Issuer CAs shall implement a process that prevents Certificates from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the Issuer CA has verified this information in accordance with the following:

Publicly-trusted OV/DV TLS/SSL:

- CA/Browser Forum Baseline Requirements; and
- Section 3.2 of the CP and this CPS.

Publicly-trusted EV

Applicant, then the certificate may be approved for issuance with notice of issuance sent to the address of record. If the photo ID does not confirm the

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

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

The Issuer CA shall verify all registration information commensurate with the requested certificate type. Acceptabl

Object Signing Certificates (including EV Code Signing Certificates)	If a Certificate names an organization, an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a Reliable Method of Communication.
Adobe Signing Certificates	If the Certifate names an organization, the requester's contact information is verified with an authoritative source within the applicant's organization using a Reliable Method of Communication. The contact information is then used to confirm the authenticity of the certificate request.
Level 1 Client Certificates - Personal or Enterprise (email certificates) issued through the native DigiCert infrastructure IGTF	An individual with control over the email address listed in the Certificate or with a person who has technical or administrative control over the domain or the email address to be listed in the Certificate.

DV and OV SSL/TLS Certificates	Username and password	According to the Baseline Requirements
EV SSL/TLS Certificates	Username and password	According to the EV Guidelines
Subscriber Code Signing Certificates (Minimum Requirements and EV)	Username and password	According to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates
Signing Authority EV Code Signing Certificates	Username and password	According to the Baseline Requirements for the Issuance and Management

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;
- Any authorized representative of an Issuer CA; or
- Any authorized representative of an RA.

No individual or entity listed on a government denied list, list of prohibited persons, or

validation chain to the ICANN root.

CAs must log actions taken based on CAA records, and document issuance prevented by CAA for feedback to the CA/Browser Forum. Issuing CAs must specify the domain names authorizing issuance in their CPS.

The Issuer CA shall ensure that all communication between the Issuer CA and an RA regarding certificate issuance or changes in the status of a Certificate are made using secure and auditable methods. If databases or other sources are used to confirm sensitive or confidential attributes of an individual subscriber, then that sensitive information shall be protected and securely exchanged in a confidential and tamper-evident manner, protected from unauthorized access, and tracked using an auditable chain of custody.

For publicly-trusted TLS Certificates, Issuer CAs shall develop, maintain, and implement documented procedures that identify and require additional verification activity for High Risk Certificate Requests prior to the Certificate's approval, as reasonably necessary to ensure that such requests are properly verified under the CABF Baseline Requirements.

The Issuer CA shall reject any certificate application that cannot be verified. The Issuer CA shall not issue Certificates containing a new gTLD under consideration but not yet approved by ICANN. The Issuer CA or RA may also reject a certificate application on any reasonable basis, including if the Certificate could damage the Issuer CA's business or reputation. Issuer CAs shall not issue certificates containing internal names. Issuer CAs are not required to provide a reason for rejecting a certificate application.

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

All parties involved in certificate application processing shall use reasonable efforts to ensure that certificate applications are processed in a timely manner. There is no time stipulation to complete the processing of an application unless otherwise indicated in the relevant Subscriber Agreement, CPS or other Agreement b

CERTIFICATE MODIFICATION

Modifying a Certificate means creating a new Certificate for the same subject with authenticated information that differs slightly from the old Certificate (e.g., changes to email address or non-essential parts of names or attributes) provided that the modification otherwise complies with this CP. The new Certificate may have the same or a different subject Public Key.

related notice to published revocation must not exceed the time frame set forth in Section 4.9.1. The date

- the request must be digitally signed or verified by DigiCert to confirm the request.

The reason code CRL entry extension must be populated with “certificateHold”.

DigiCert sets the maximum time period an EPCS certificate may be in suspension to 30 days. If the Certificate remains in suspension throughout the period, the requestor has until the 30th day to confirm unsuspension or it shall be revoked.

DigiCert shall maintain an internal policy to ensure the certificates do not remain in suspension beyond the 30-day time limit.

If the subscriber has not removed the certificate from hold

following reasons:

1. The [illegible]

5.1. PHYSICAL CONTROLS

unauthorized physical access. Each Issuer CA and each RA shall duplicate and store its audit and archive information in a backup location that is separate from its primary operations facility.

Paper waste containing sensitive data shall be shredded before disposal. Sensitive data on magnetic or other digital media must be permanently erased before disposal

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

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

5.2 PROCEDURAL CONTROLS

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

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

5.2.1.1 CA Administrators

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

5.2.1.2 Registration Officers – CMS RA, Validation and Vetting Personnel

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

5.2.1.3 System Administrator/ System Engineer (Operator)

The System Administrator, System Engineer, or CA Operator is responsible for installing and configuring critical CA system hardware. The System Administrator / Engineer is also responsible for keeping systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4 Internal Auditor Role

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

5.2.1.5 RA Administrators

RA Administrators install, configure and manage the RA software.

Checks of previous residences are over the past three years. All other checks are for the prior five years. The Issuer CA or RA shall verify the highest education degree obtained regardless of the date awarded and shall refresh all background checks at least every five years. Based upon the information obtained, a competent adjudication authority within the Issuer CA or RA shall adjudicate whether the individual is suitable for the position to which they will be assigned.

The Issuer CA shall provide skills training in the Issuer CA's PKI operations for the personnel performing information verification duties including:

1. Basic Public Key Infrastructure (PKI) knowledge;
2. Software versions used by the Issuer CA;
3. Authentication and verification policies and procedures;
4. CA/RA

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

5.4 AUDIT LOGGING PROCEDURES

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

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

No stipulation.

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

5.5 RECORDS ARCHIVAL

The Issuer CA shall comply with any record retention policies that apply by law and retrieved as necessary by request of authorized parties. The Issuer CA shall include sufficient detail in archived records to show that a Certificate was issued in accordance with the CPS.

Issuer CAs and each Delegated Third Party shall archive records related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party SG[12 792 reW*nBT/F1 9.96 Tf0.94118 0 0 1 117.98 636.22 Tm0 g0 G[( )] TJETQq(De)-.96 Tfti5rnageme

17. Access to Private Keys for key recovery purposes,
18. Changes to trusted Public Keys,
19. Export of Private Keys,
20. Approval or rejection of a revocation request,
21. Appointment of an individual to a trusted role,
22. Destruction of a cryptographic module,
23. Certificate compromise notifications,
24. Remedial action taken as a result of violations of physical security, and
25. Violations of the CP or CPS.

For TLS certificates, Issuer CAs and each Delegated Third Party shall retain, for at least two (2) years:

1. CA certificate and key lifecycle management event records (as set forth in section 5.4.1) ; after the later occurrence of:
   1. the destruction of the CA Private Key; or
   2. the revocation or expiration of the final CA Certificate in that set of Certificates that have an X.509v3 `basicConstraints` extension with the `cA` field set to true and which share a common Public Key corresponding to the CA Private Key;
2. Subscriber Certificate lifecycle management event records (as set forth in section 5.4.1 after the expiration of the Subscriber Certificate;
3. All security event records (as set forth in [Section 5.4.1 after the event occurred;
4. All archived records and documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and Delegated Third Party Systems (as set forth in Section 5.5.1); and
5. All archived records and documentation relating to the verification, issuance, and revocation of certificate requests and Certificates after the later occurrence of:
   1. such records and documentation were last relied upon in the verification, issuance, or revocation of certificate requests and Certificates; or
   2. the expiration of the Subscriber Certificates relying upon such records and documentation.

For all other Certificates, the Issuer CA shall retain archived data for at least 7.5 years or according to their respective requirements and as contractually agreed upon.

The Issuer CA shall store its archived records at a secure off-site location in a manner that prevents unauthorized modification, substitution, or destruction. No unauthorized user may access, write, or delete the archives. If the original media cannot retain the data for the required period, the archive site must define a mechanism to periodically transfer the archived data to new media. The Issuer CA shall ensure that all archived information can be obtained within a reasonable timeframe through specified recovery services.

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

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

The Issuer CA shall collect archive information internally.

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

The Issuer CA may allow Subscribers to obtain a copy of their archived

If the Issuer CA suspects that a CA Private Key is compromised or lost then the Issuer CA shall

Relying Parties as:

- Specified in a certificate validation or path discovery policy file;
- Trust anchors in commercial browsers and operating system root stores; and/or
- Roots signed by other CAs.

The Issuer CA may distribute Public Keys that are part of an updated signature Key Pair as a self- signed Certificate, as a new CA Certificate, or in a key roll-over Certificate. All accreditation authorities supporting DigiCert Certificates and all application software providers are permitted to redistribute any Root Certificate that is issued under this CP.

For signing Certificates, the Issuer CAs shall use:

- 2048-bit or greater RSA Key (with a modulus size in bits divisible by 8);
- 256-bit ECDSA Key or greater with the matching Secure Hash Algorithm as required and a valid point on the elliptic curve; or
- A hash algorithm that is equally or more resistant to a collision attack allowed by the Mozilla Root Store policy and other references in sections 1.1 and1.6.3.

The Issuer CA shall only issue end-entity Certificates that contain at least 2048-bit Public Keys for RSA, or 224 bits for elliptic curve algorithms. The Issuer CA may require higher bit keys in its sole discretion if it is allowed by the programs and policies listed in section 1.1 and 1.6.3.

Any Root Certificates participating in the AATL program must be at least 3072-bit for RSA and 384-bit for ECDSA when issued on or after July 1, 2017.

-7(v 1.)4(20)-11(17.)] 17 Tm0 g0 G[(Ke)-9(.00216 Tm0 g0 G[( )] TJETQq0.00000912 0 612 792 reW*nBT/F1 9.96 Tf0.94118 0 0 1 219.41 56(J)

1. Be generated

Techniques that MAY be used to satisfy this requirement include:

1. Use of an HSM, verified by means of a manufacturer's certificate;
2. A cloud-based key generation and protection solution with the following requirements:
    a. Key creation, storage, and usage of Private Key must remain within the security boundaries of the cloud solution's Hardware Crypto Module that conforms to the specified requirements;
    b. Subscription at the level that manages the Private Key must be configured

an unauthorized person or an organization not affiliated with the Subordinated CA, then the Issuer CA will revoke all certificates that include the Public Key corresponding to the communicated Private Key.

Issuer CAs pre-generating private keys and transferring them into a hardware token, for example transferring generated end-user Subscriber private keys into a smart card, shall securely transfer such private keys into the token to the extent necessary to prevent loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys.

The Issuer CA shall store its CA Private Keys on a cryptographic module which has been evaluated to at least FIPS 140-2 Level 3. Issuer CA or RA private keys held on hardware cryptographic modules shall be stored in encrypted form.

The Issuer CA shall activate its Private Keys in accordance with the specifications of the cryptographic module manufacturer.

Subscribers are solely responsible for protecting their Private Keys in a manner commensurate with the Certificate type. At a minimum, Subscribers must authenticate themselves to the cryptographic module before activating their Private Keys. Entry of activation data shall be protected from disclosure.

Subscribers should also take commercially reasonable measures for the physical protection of their workstation to prevent use of thef1 0 0 1 243.53 599.38 Tm0 g0 G[(C)19(r)15(y)9(p)10(t)6(o)15(g)9(r)15(1 256.

When passwords are required, Subscribers shall generate passwords that meet the requirements specified by the CAB Forums Network Security Requirements.

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

- Memorized;
- Biometric in nature; or
- Recorded and secured at the level of assurance associated with the activation of the cryptographic module, and shall not be stored with the cryptographic module.

The Issuer CA shall require personnel to memorize

2. Manage privileges to limit users to their assigned roles;
3. Enforce domain integrity boundaries for security critical processes; and
4. Support recovery from key or system failure.

A CMS must have the following computer security functions:

1. Authenticate the identity of users before permitting access to the system or applications;
2. Manage privileges of users to limit users to their assigned roles;
3. Generate and archive audit records for all transactions (see Section 5.4);
4. Enforce domain integrity boundaries for security critical processes; and
5. Support recovery from key or system failure.

Issuer CAs shall enforce multi-factor authentication on any account capable of

6.7 NETWORK SECURITY CONTROLS

Issuer CA and RA functions are performed using networks secured in accordance with the standards documented in this CP to prevent unauthorized access, tampering, and denial-of-service attacks.

Communications of sensitive information shall be protected using point-to-point encryption for confidentiality and digital signatures for non-repudiation and authentication.

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

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

6.8 TIME-STAMPING

Certificates, CRLs, and other revocation database entries shall contain time and date information. Such time information need not be cryptographic based.

Issuer CAs shall ensure that the accuracy of clocks used for time-stamping are within three minutes. Electronic or manual procedures may be used to maintain system time. Clock adjustments are auditable events, see Section 5.4.1.

CERTIFICATE PROFILE

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

Issuer CAs shall issue X.509 version 3 Certificates.

ecdsa-with-SHA224	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 1 }
ecdsa-with-SH256	{ iso(1)

7.1.5.1 Name-Constrained serverAuth CAs

If the Subordinate CA Certificate includes the id-kp-serverAuth extended key usage, then a technically constrained Subordinate CA Certificate shall include the Name Constraints X.509v3 extension with constraints on dNSName, iPAddress and Directory Name as follows:

a) For each dNSName in permittedSubtrees, the Issuer CA shall confirm that the Applicant has registered the dNSName or has been authorized by the domain registrant to act on the registrant's behalf in line with the verification practices of Baseline Requirements section 3.2.2.4.

b) For each iP Address range in permitted Subtrees, the Issuer CA shall confirm that the Applicant has been assigned the iP Address range or has been authorized by the assigner to act on the assignee's behalf.

c) For each DirectoryName in permitted Subtrees the Issuer CA shall confirm the Applicant's and/or Subsidiary's Organizational name(s) and location(s) such that end entity certificates issued

8

or software.

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

REPRESENTATIONS AND WARRANTIES

Issuer CAs must represent to DigiCert, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP and their CPS. Subscriber Agreements may include additional representations and warranties that do not contradict or supersede this CP.

At a minimum, Issuer CAs shall require RAs operating on their behalf to represent that they have followed this CP

or as limited by law, DigiCert disclaims all warranties and obligations related to this CP.

LIMITATIONSOFLIABILITY

Issuer CAs may limit their

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

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.

GOVERNING LAW

For