Cerner Direct HISP

Welcome to Cerner Direct!

Congratulations on taking the first steps toward utilizing Cerner Direct for simple and secure exchange of health care information. The Cerner Direct Health Information Service Provider (“HISP”) is a full service HISP, compliant with national Direct Project standards and accredited through the Direct Trusted Agent Accreditation Program (DTAAP).

This application packet includes a **Cerner Direct HISP Application**. This application aligns with industry expectations that all trusted professional Directed exchange participants are part of an organization that is either (i) a HIPAA covered entity or a business associate, or (ii) a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. The end outcome is to establish a unique digital identity of the Subscriber. This is accomplished by issuing a digital certificate, which is subsequently used as a unique “signature” to ensure authenticity of any information being communicated via Cerner Direct by the Subscriber. Therefore, it is important for Cerner’s Registration Authority, DigiCert, to first verify the authenticity of the Subscriber and the Authorized Representative making the request by utilizing the information you will provide in the DigiCert Declaration of Identity agreement (sample available at www.cerner.com/cps).

After you successfully complete the Cerner Direct HISP and DigiCert Declaration of Identity application processes, you will become a Cerner Direct Subscriber, and your organization’s Direct addresses will be universally accepted by trusted recipients across the nation.

Instructions

Step 1: Complete the **Cerner Direct HISP Application** for the production Direct domain being requested and submit to Cerner. The form must be signed by an Authorized Representative. Submit completed form to eService (Solution Family of Community & Consumer Health, Solution of Cerner Direct). If you do not have access to eService, please contact your distributing partner for submission on your behalf or call Cerner Client Care at 1-866-221-8877 Option 6 and mention Cerner Direct Messaging and request to email the application in to be added as an SR attachment. Keep the original completed Application for your records.

Step 2: Once submitted to Cerner and processed for certificate request, you will be contacted shortly thereafter by DigiCert, our Registration Authority, to complete and submit the Declaration of Identity agreement to verify personal identity. Upon successful completion of these steps, you will be notified of a Direct certificate issuance.

For more information, visit Cerner Direct on uCern.

Submit completed form to eService (Solution Family: Community & Consumer Health, Solution: Cerner Direct). If you do not have access to eService, please contact your distributing partner for submission on your behalf or call Cerner Client Care at 1-8666-221-8877 Option 6 and mention Cerner Direct Messaging.

Cerner Direct HISP Application

Once submitted to Cerner and processed, you will be contacted by Cerner's trusted partner, DigiCert, for completion of their Declaration of Identity form (sample available from http://www.cerner.com/cps) to confirm the Authorized Representative's identity per DirectTrust standards.

Organization Information

Legal Business Name: Wisconsin Department of Corrections		
Mailing Street Address: 3099 East Washington Ave		
City: Madison	State: WI	Zip: 53704

Healthcare Category

If you are not a Covered Entity as defined by HIPAA, select one (no selection indicates Covered Entity Status):

□ Business Associate as defined by HIPAA

□ Non-HIPAA Healthcare Entity defined as an entity that has an appropriate healthcare-related need to exchange Direct messages and which agrees to handle protected health information with privacy and security protections that are at least as protective as those required by HIPAA.

Direct Email Domain

The following Direct email domain has been selected for your organization:
Prod @widoc.cernerdirect.com
NonProd @ widoc .stagingcernerdirect.com

Authorized Representative Contact Information

First Name: Cathy	Last Name: Jess
Business Email: cathy.jess@wisconsin.gov	Phone: 608 240-5055

Primary Contacts for Cerner Direct Notifications (optional)

Name: Robert Beaverson	Phone: 608 240-5640	Email: docdldmsbtmemrbusinessanalysts@wisconsin.gov

Authorized Representative Signature

Subscriber's use of Cerner Direct is subject to the parties' agreements in Contract Number 410008-M16-EB4253A-RFP-01, effective June 28, 2016,and the Certification Practice Statement, which is available at http://www.cerner.com/cps and the Cerner Direct Terms of Use available at https://cernerdirect.com/mail/termsofuse.action.

Subscriber warrants: (i) the information contained herein is true and accurate, (ii) it will comply with all applicable federal and state privacy laws, including but not limited to HIPAA, (iii) the information provided above does not infringe on the intellectual property rights of another person or entity including any trademarks associated with the requested Direct email domain, (iv) it will limit access to employees, subcontractors or agents of the Subscriber and Subscriber's Affiliates engaging in "Treatment," "Payment," and "Health Care Operations" as defined by HIPAA, each such employee, subcontractor or agent who is authorized by Client to use Cerner Direct shall be an "End User", and (v) it will promptly remove an End User's access to Cerner Direct upon (a) an End User leaving their practice or organization, (b) an End User violating any of the Cerner Direct Terms of Use, (c) reasonable request by Cerner, or (d) any event otherwise deemed appropriate by the Subscriber. Subscriber agrees to notify Cerner (y) of any actual or suspected abuse or misuse of Cerner Direct, and (z) in advance and in writing, of any changes to Subscriber's "Healthcare Category" selected above. Affiliate shall mean any company controlled by, controlling or under common control with Licensee. For purposes of this definition, "control" means the possession, directly or indirectly, of the power to direct or cause the direction of the management and policies of such person or entity, whether through ownership of more than fifty percent (50%) of the outstanding voting securities or other interests, or by contract.

I, as the Authorized Representative, am authorized to act in the name of the Subscriber and represent that I am an employee or agent of the Subscriber. You understand that before you may use Cerner Direct, you must successfully complete this application and subsequently DigiCert's Declaration of Identity application, which includes confirmation of your identity, as required by DirectTrust.

Signature:	
Print Full Legal Name: Cathy A Jess	
Title: Deputy Secretary	Date:

Cerner Direct

Terms of Use

Cerner Direct is offered to you by Cerner Corporation ("Cerner"). Your use of *Cerner Direct* is governed by these terms of use ("Terms"), and by using or accessing *Cerner Direct* you agree to be bound by them. If you do not agree to these Terms, you may not use *Cerner Direct*. In certain circumstances Cerner may have a separate agreement directly with you or your system administrator governing your use of *Cerner Direct*; in the event of any conflict between these Terms and terms of such other agreement, the terms of such other agreement shall prevail.

Creating and Accessing Your Account

Your system administrator, such as your employer or a health information exchange or an accountable care organization, will assign your *Cerner Direct* account to you.

You may not permit any other person to access your account using your user name and password. The security of your password and the use of your account is your responsibility. If you learn or suspect that your user name or password has been wrongfully used or disclosed, you should promptly notify Cerner and your system administrator and immediately reset your password. To help ensure the security of your password or account, please sign out of your account at the end of each session. You must be at least 18 years old to establish an account.

You are responsible for ensuring your account information is current, accurate, and complete.

Cerner Direct Service

Information Exchange. *Cerner Direct* is designed to enable the secure exchange of healthcare-related information between providers and organizations engaged in providing care and consumers receiving care. Cerner is not responsible for the timeliness, deletion, mis-delivery or failure to store any communications or personalization settings within, by or through *Cerner Direct*. *Cerner Direct* is not a replacement for an electronic medical record and is not for use in emergencies. In the event of a true emergency, you should use another means of communication.

Prohibited Activities. You may not use *Cerner Direct* for any prohibited activities. By way of example, and not as a limitation, you agree that when using *Cerner Direct*, you will not:

- Defame, abuse, harass, stalk, threaten, damage the reputation of or otherwise infringe or violate the legal rights (such as rights of privacy and publicity) of others; breach any legal duty owed to others nor advocate, promote or incite any third party to commit or assist any unlawful or criminal act.
- Publish, post, upload, transmit, distribute or disseminate any inappropriate, profane, defamatory, infringing, obscene, offensive, discriminatory, indecent, illegal or unlawful topic, name, material or information.
- Intentionally transmit or distribute inaccurate, false or misleading information or information containing your personal opinions not genuinely held by you.
- Upload files that contain software or other material protected by intellectual property laws (or by rights of privacy of publicity) unless you own or control the rights thereto or have received all necessary consents.
- Publish, post, transmit, upload or distribute another's confidential, proprietary, sensitive or personal information or any information relating (directly or indirectly) to any past or existing commercial arrangements, contracts, engagements or provision of goods and services between any persons or organizations which is in violation of any arrangements, contracts, engagements, professional rules of ethics or any applicable law or regulation.
- Intentionally upload files that contain viruses, worms, corrupted files, or any other similar software, programs or malicious content that may damage the operation of systems hosting *Cerner Direct* or another's computer.
- Advertise or offer to sell or buy or make available any goods or services for any business purpose, unless *Cerner Direct* specifically allows such messages in which case you shall not advertise or offer to sell or buy or make available any unlawful goods or services.
- Influence or attempt to influence, for commercial purposes, (through economic incentives or otherwise) any diagnostic or treatment-related decisions of a healthcare provider.
- Conduct or forward surveys (unrelated to your business), contests, pyramid schemes or chain letters.
- Generate or facilitate unsolicited commercial email ("spam").
- Download any file posted by another user of *Cerner Direct* that you know, or reasonably should know, cannot be legally distributed in such manner.
- Falsify or delete any author attributions, legal or other proper notices or proprietary designations or labels of the origin or source of software or other material contained in a file that is uploaded.
- Restrict or inhibit any other user from using and enjoying *Cerner Direct*.
- Violate any applicable laws or regulations.

Communication Tool. *Cerner Direct* is provided as a communication tool only. It is your responsibility to ensure that you (i) comply with all applicable laws, rules and regulations as you use Cerner Direct, (ii) comply with any policies and procedures imposed by your system administrator, if applicable, regarding your use of *Cerner Direct* and (iii) obtain all appropriate and necessary consents to use or disclose any personally identifiable information in compliance with all federal and state privacy laws, including but not limited to the Health Insurance Portability and Accountability Act ("HIPAA").

Viruses. Cerner takes commercially reasonable measures to check that messages sent through *Cerner Direct* are free from viruses and other malicious computer instructions, devices or techniques ("Viruses"), however, Cerner does not guarantee the messages have not been infected with a Virus. It is your responsibility to protect your computer systems from Viruses.

Record Retention and Classification. *Cerner Direct* is not a medical record. It is your responsibility to ensure that messages sent through *Cerner Direct* are incorporated into a patient's medical record as necessary. Termination of your account will result in permanent deletion of all messages contained within your account. You are responsible for creating and maintaining your own records retention policy for *Cerner Direct* messages.

Operation and Termination. Cerner reserves complete and sole discretion with respect to the operation of *Cerner Direct*. Cerner may, among other things, delete email if it has not been accessed by a user within the time established by any posted Cerner policies. Cerner will not review the contents of email except as required or allowed by applicable law or legal process.

Cerner may terminate or suspend your access to *Cerner Direct* and may delete your personal account, at any time, without providing notice to you. Any such termination or suspension may be subject to the terms of other applicable agreements (i) directly between you and Cerner, or (ii) between your system administrator and Cerner.

Participating in the Directory

Your system administrator may enable your participation in a Health Care Directory ("Directory"), which contains information about individuals outside of your organization (such as name, title and practice specialty) in an effort to facilitate your communication with them. If you use the Directory, you agree not to:

- Copy, or allow to be copied, the information contained in the directory.
- Sell the information contained in the directory.
- Disclose the information contained in the directory.
- Use, or allow use of, the directory for direct marketing, database marketing, telemarketing, marketing analysis, or research purposes.

Use of the Directory is subject to the Directory Terms available here.

Disclosure of Information

Cerner may, in Cerner's sole and reasonable discretion, disclose any information necessary to satisfy applicable law, regulation, legal process or governmental request.

Privacy

You agree to the terms and conditions of the Privacy Policy, which is hereby incorporated into and made part of these Terms.

No Warranties; Limitation of Liability

Cerner Direct is a communication tool only. You are responsible for any acts or omissions relating to your use of *Cerner Direct* and for any damages incurred as a result thereof. *CERNER DIRECT* IS PROVIDED TO YOU "AS IS" WITHOUT WARRANTY OF ANY KIND. CERNER DOES NOT WARRANT THE RELIABILITY OR AVAILABILITY OF *CERNER DIRECT*, NOR DOES CERNER GUARANTEE THAT *CERNER DIRECT* WILL BE ERROR-FREE OR UNINTERRUPTED OR THAT DEFECTS WILL BE CORRECTED. TO THE EXTENT PERMITTED BY LAW, CERNER AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS AND IMPLIED. TO THE EXTENT PERMITTED BY LAW, NEITHER CERNER NOR ITS SUPPLIERS WILL BE RESPONSIBLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, EXEMPLARY, OR PUNITIVE DAMAGES, OR LOST PROFITS, REVENUES OR DATA. NEITHER CERNER NOR ITS SUPPLIERS WILL BE LIABLE TO YOU FOR ANY DAMAGES EXCEEDING THE GREATER OF (A) THE FEES YOU PAID FOR USE OF CERNER DIRECT, OR (B) ONE THOUSAND DOLLARS. IF YOU ARE DISSATISFIED WITH *CERNER DIRECT*, OR WITH THESE TERMS, YOUR SOLE AND EXCLUSIVE REMEDY IS TO DISCONTINUE USING *CERNER DIRECT*.

Indemnification

YOU AGREE TO INDEMNIFY, DEFEND, AND HOLD CERNER AND ITS SUPPLIERS HARMLESS FROM AND AGAINST ALL CLAIMS, DAMAGES, AND EXPENSES ("CLAIMS") ARISING OUT OF OR RELATED TO YOUR USE OF *CERNER DIRECT*, OTHER THAN THOSE CLAIMS ARISING OUT OF OR RELATED TO CERNER'S NEGLIGENCE OR WILLFUL MISCONDUCT IN PROVIDING *CERNER DIRECT*.

Feedback

Cerner welcomes your suggestions to improve *Cerner Direct*. If you provide feedback to Cerner, you agree that such feedback, including all ideas and concepts within the feedback, shall be the property of Cerner and you assign to Cerner your ownership rights in the feedback.

Notices

Cerner may deliver notice to you by means of electronic mail, a general notice on Cerner's website, or by written communication delivered by first class U.S. mail to your address on record within your account in Cerner's account information. You may give notice to Cerner at any time by letter delivered by first class postage prepaid U.S. mail or overnight courier to the following address:

Cerner Corporation
2800 Rockcreek Parkway
Kansas City, Missouri 64117 U.S.A.
Attention: Chief Legal Officer

General

These terms are governed by the laws of the State of Missouri, U.S.A. You consent to the exclusive jurisdiction and venue of courts in Clay County, Missouri, U.S.A. in all disputes arising out of or relating to your use of *Cerner Direct*. Any cause of action or claim you may have with respect to Cerner or its suppliers must be commenced within one (1) year after the claim or cause of action arises. Cerner's failure to enforce strict performance of any provision of these Terms shall not be construed as a waiver of any provision or right. Cerner may assign its rights and duties to any party at any time without notice to you.

Cerner's performance of these Terms is subject to existing laws and legal process, and nothing contained in these terms is in derogation of Cerner's obligation to comply with governmental, court and law enforcement requests or requirements relating to your use of *Cerner Direct* or information provided to or gathered by Cerner with respect to such use. If any part of these Terms is determined to be invalid or unenforceable then the invalid or unenforceable provision shall be superseded by a valid, enforceable provision that most closely matches the intent of the original provision and the remainder of these Terms shall continue in effect. Unless specified otherwise as you use Cerner Direct, these Terms constitute the entire agreement between you and Cerner with respect to *Cerner Direct* and these Terms supersede all prior or contemporaneous communications and proposals, whether electronic, oral, or written, between you and Cerner with respect to *Cerner Direct*.

Modification of Terms

Cerner may change these Terms at any time without advance notice to you. You are responsible for regularly reviewing these Terms. Your continued use of *Cerner Direct* constitutes your acceptance of the revised terms.

Last Modified: March 9, 2016

RIVACY POLICY TERMS OF USE CONTACT US

Health Care Directory Policy

Organizations who sign up to use Cerner Direct ("**Subscriber**") may contribute to and use the Health Care Directory (the "**Directory**"). The Directory is a consolidated listing of information about individuals who participate in one or more health care information exchange community(ies) (such as DirectTrust) ("**Participant**"). The purpose of the Directory is to better facilitate health care information exchange between providers. Subscribers must contribute Participant information to the Directory to have access to it.

How to Contribute to the Directory

A Subscriber may proactively choose to contribute its information into the Directory or Cerner may choose populate the Directory itself with information that is made available to it by the Subscriber. Subscribers may contribute information by using the administrative capabilities Cerner has provided. If a Subscriber does not wish to have its information contributed to the Directory it can opt-out, at any time, by logging a service request to Cerner's support organization requesting to not contribute to the Health Care Directory. Regardless of how information is contributed, Subscribers are responsible for managing all Directory contributions.

Directory Information

The following minimum Participant information will be made available within the Directory: Participant full name, Direct email address, National Provider Identifier (if applicable), business address, and the Subscriber name. Additional information, such as provider specialty, may be available within the Directory as elected by the Subscriber. The Subscriber is the authoritative source of all Participant information published in the Directory and is solely responsible for keeping the information accurate and complete. Participants must contact the Subscriber to make necessary updates to their information. Cerner updates the Directory on a daily basis.

Directory Usage

Participants may use the information from the Directory solely for the purposes of supporting the exchange of health care information from within Cerner's solutions (e.g. Cerner Millennium, Cerner Direct). Participants may search the Directory and save search results in a local address book, made available within Cerner's solutions. Subscribers may choose to store local copies of information obtained from the Directory; in such an event the Subscriber is responsible for regularly synchronizing the local copies with updates made by Cerner to the Directory at a recommended interval of every 24-48 hours.

If a Participant receives unwanted messages, the Participant must notify the sender of his/her desire to stop receiving the unwanted messages. Cerner does not control these messages.

Directory Restrictions

Subscriber and Participant agree not to:

- Copy, or allow to be copied, the information contained in the Directory (other than as specifically allowed under the paragraph entitled "Directory Usage" above);
- Sell the information contained in the Directory;

- Disclose the information contained in the Directory outside of the Subscriber organization;
- Use, or allow use of, the Directory for direct marketing, database marketing, telemarketing, marketing analysis, or research purposes;
- Intentionally transmit or distribute inaccurate, false or misleading information;
- Advertise or offer to sell, buy or make available any goods or services for any business purpose, unless Cerner specifically allows such messages in writing (provided however, that in no event may Subscriber or a Participant advertise, offer to sell, buy or make available any unlawful goods or services or any goods or services for an unlawful purpose);
- Influence or attempt to influence, for commercial purposes (through economic incentives or otherwise) any diagnostic or treatment-related decisions of a healthcare provider;
- Conduct or forward surveys (unrelated to your business), contests, pyramid schemes or chain letters;
- Generate or facilitate unsolicited commercial email, spam or mass mailing; or
- Violate any applicable laws or regulations.

DirectTrust Directory

One of the communities Cerner participates in is DirectTrust. As a member of that community, Cerner is required to uphold the expectations set forth in the DirectTrust Directory Data Sharing Policy ("**DirectTrust Directory Policy**") available at https://www.directtrust.org/about-policies/. This Policy shall at all times be interpreted in accordance with the DirectTrust Directory Policy.

Termination of Directory or Directory Access

Cerner may, in its sole discretion, (i) terminate or suspend a Subscriber's access to the Directory for violation of this policy, or (ii) terminate or suspect its provision of the Directory to all Subscribers and Participants. Cerner will take reasonable steps to notify you of any such termination or suspension.

Modification of Terms

Cerner may change these Terms at any time without advance notice to you. You are responsible for regularly reviewing these Terms. Your continued use of the Directory constitutes your acceptance of the revised terms.

Last Modified: March 9, 2016

Introduction

For uninterrupted Directed exchange to occur, it takes both technology and policy. The Cerner Direct HISP (Health Information Service Provider) combines the technology of the Direct Project standards with the policy and best practices defined by DirectTrust.org. By industry terms, it is a full-service HISP providing the transport for Direct messages as well as Registration Authority and Certificate Authority services. Direct certificates are issued at the Organization level and follow the processes documented in our Certificate Practices Statement.

The Cerner Direct HISP is the mechanism used to provision users with a Direct email address. The Cerner Direct HISP provides the infrastructure necessary to manage message encryption, the parties who can be communicated with, and the incorporation of appropriate policies and procedures necessary to ensure a level of confidence in provisioning members on the network appropriate to health care.

For more information, visit the Cerner Direct uCern Group on uCern Connect.

Cerner Direct Terminology

CA (Certificate Authority) - An entity that issues digital certificates. The digital certificate certifies the ownership of a public key by the named subject of the certificate. This allows others (relying parties) to rely upon signatures or assertions made by the private key that corresponds to the public key that is certified. In this model of trust relationships, a CA is a trusted third party that is trusted by both the subject (owner) of the certificate and the party relying upon the certificate. Cerner utilizes a third party agency that is DTAAP accredited and acts the CA for the Cerner Direct HISP.

CAMM (CareAware Multimedia) - Cerner's enterprise storage solution for PACS and Digital Objects

CDA (Cerner Direct Administrator) - Each organization using the Cerner Direct Web Inbox will have an CDA who is responsible for sending invitations to people within their organization(s) that are authorized to have a Cerner Direct web mailbox. The CDA will have access to https://cernerdirect.com/administration. Could also mean Clinical Document Architecture (an HL7 standard).

CDG (Cerner Document Generator) - The Clinical Document Generator is a service that generates an HL7 Continuity of Care Document (CCD) for a given patient or encounter.

CPS (Certification Practice Statement) - A public statement describing the practices that a Certification Authority employs for issuing, renewing, revoking and validating Digital Certificates and for supporting reliance on Certificates. A CPS expands on the Certificate Policies of a particular Certification Authority. In Cerner's case, our past and third party's current CPS is accessible through http://www.cerner.com/cps and complies with the DirectTrust.org Certificate Policy.

Digital Certificate (also known as a Certificate or Direct Certificate) - A digital representation of information which:

1. Identifies the Certification Authority issuing it
2. Names or identifies its Subscriber
3. Contains the Subscriber's Public Key
4. Identifies its operational period
5. Is digitally signed by the Certification Authority issuing it.

Cerner Direct HISP leverages a third party CA to issue X.509 digital certificates at the Organization level per the CPS. The Direct specification requires digital certificates for encrypting and decrypting Direct messages, signing Direct messages, and verifying trust of Direct messages.

DSN (Disposition Status Notification) - A DSN is commonly referred to as a bounce message. It is a email message that complies with RFC 3464.

DTAAP (Directed Trusted Agent Accreditation Program) - A national accreditation program for health information — trusted agent — service providers, including health information service providers (HISPs), certificate authorities (CAs) and registration authorities (RAs). The purpose of this program is to establish trust between Direct entities. Electronic Healthcare Network Accreditation Commission (EHNAC) partnered with DirectTrust.org and created DTAAP. The Cerner Direct HISP is DTAAP accredited as a HISP and utilizes a third party CA that is a DTAAP accredited RA and CA.

HISP (Health Information Service Provider) - An entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital certificate. Acting in the capacity of an agent for the Subscriber, the HISP may hold and manage PKI private keys associated with a Direct digital certificate on behalf of the Subscriber. The HISP for all Direct-enabled Cerner solutions is Cerner Direct.

MDN (Message Disposition Notification) - An MDN is commonly referred to as a read receipt. It is an email message that complies with RFC 3798.

PKI (Public Key Infrastructure) - Set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates

RRD (Remote Report Distribution) - Millennium solution which automatically sends clinical reporting to predefined destinations; traditionally fax stations but now can use secure email via the Cerner Direct HISP.

S/MIME (Secure/Multipurpose Internet Mail Extensions) - Used to encrypt message content while in transit.

SMTP (Simple Mail Transfer Protocol) - The Internet standard for electronic mail (email) transmission used by Network Messaging.

TPO (Treatment, Payment, and Health Care Operations) - Our Certificate Policy guarantees that the work of a trusted organization is involved with TPO.

X.509 - A widely used standard for defining digital certificates. Current version is X.509 version 3. See Digital Certificate.

Major Features

- Uses safe, HIPAA-compliant communication methods.
- Based on latest available Direct Project standards for sending and receiving of encrypted messages for purposes for treat, payment, or health care operations with recipients using any trusted Direct Project compatible system.
- Supports transport of a wide variety of content (for example, CCDs, images, plain text) between people and system-level endpoints or both.
- Includes familiar email standards, such as read receipts, bounce messages, and multiple recipient addressing (for example, To, CC).

Services

Provisioning Service

Cloud-based Web service to allow authorized service clients to register Direct addresses for their authorized Direct email domains. (For more information, see Troubleshoot Provisioning Service for Cerner Direct HISP.)

Outbound Messages Service

Cloud-based Web service to allow authorized service clients to send messages that are compliant with RFC5322 and the Direct Project Applicability Statement. (For more information, see Troubleshoot Outbound Messages for Cerner Direct HISP.)

Inbound Message Routing

The Cerner Direct HISP will push inbound messages to a web service hosted within the Direct email domain owner's system.

This page includes links to external resources. These resources are provided for reference purposes and should be used with caution. Contact your Cerner support team for more information about third-party content.

Updated April 12, 2017

CERTIFICATE SERVICES AGREEMENT

By accepting a Purchase Schedule that incorporates this Certificate Services Agreement, together with any referenced exhibits, appendices, attachments, terms and schedules, (collectively the "**Agreement**"), the entity or person accepting the Agreement ("**Customer**") is entering into a legally valid and enforceable agreement with DigiCert, Inc., a Utah corporation ("**DigiCert**"). DigiCert is a trusted third-party certification authority and experienced provider of ITU X.509 v.3 digital certificates ("**Certificates**"). DigiCert operates a web-based interface and related API that facilitates and simplifies management of Certificates. Customer desires to use a DigiCert system account and API (collectively, "**Account**") to obtain and manage Certificates containing subject information (e.g., domain names) which Customer is authorized to use.

1. Certificates.

1.1. Account Access. Subject to Customer's compliance with the terms and conditions of this Agreement, DigiCert hereby grants Customer a license to use the Account, through either the API or DigiCert's provided web interface, to order and approve Certificates for use by Customer, an affiliate of Customer, or a third party who is providing IT services to Customer's operations. This Agreement applies to each Certificate issued to Customer, regardless of (i) the Certificate type (client, code signing, or TLS/SSL), (ii) when the Customer requested the Certificate, or (iii) when the Certificate issues. This Agreement constitutes the subscriber agreement, as required under industry standards, for all Certificates issued through the Account. Customer must maintain security over access to the Account. Customer is liable for any use of the Account by individuals obtaining access credentials from Customer. Customer will not scan a DigiCert IP address without obtaining DigiCert's prior written consent. DigiCert reserves the right to block an IP address that DigiCert believes has been used to initiate a scan without such consent. DigiCert may throttle any access to the Account if DigiCert believes a system has initiated excessive connections to DigiCert's services.

1.2. Account Users. Customer authorizes each individual listed as an administrator in the Account to act as a Certificate Requester, Certificate Approver, and Contract Signer (as defined in the EV Guidelines) and to communicate with DigiCert regarding the management of Certificates and key sets. **"EV Guidelines"** means the Extended Validation Guidelines published by the CA/Browser Forum and made publicly available at www.cabforum.org . Customer may revoke this authority by sending notice to DigiCert. Customer is responsible for periodically reviewing and reconfirming which individuals have authority to request and approve Certificates. If Customer wishes to remove an account user, then Customer will take the steps necessary to prevent the user's access to the Account, including changing its password and other authentication mechanisms. Customer must notify DigiCert immediately if any unauthorized use of the Account is detected.

1.3. Certificates. Customer will order and use Certificates in accordance with the Certificate Terms of Use which are available at https://www.digicert.com/certificate-terms.htm, which terms are hereby incorporated by reference.

1.4. Accurate Information. Customer will notify DigiCert within 5 Business Days if any information relating to the Account changes. "**Business Day**" means Monday through Friday, excluding U.S. Federal Holidays, which are set forth in 5 U.S.C. § 6103. Customer will respond to any inquiries from DigiCert regarding the validity of information provided by Customer within 5 Business Days after Customer receives notice of the inquiry.

2. Fees.

2.1. Fees. Customer will pay DigiCert the fees posted in Customer's Account or set forth in the Purchase Schedule for Certificates. Prices of Certificates available for purchase on a per-Certificate basis are subject to change; updates to pricing will be posted in Customer's Account prior to purchase. All payments are due and payable either within 30 days of the date of purchase or such other period, if any, stated in the Purchase Schedule. This fee is for the services provided by DigiCert and is not a royalty or license fee. DigiCert may suspend or limit Customer's access to the Account without notice if Customer fails to pay the fees when due.

2.2. Purchase Schedule. "**Purchase Schedule**" means the ordering document, invoice, purchase order or other order form accepted by Customer to purchase Certificates. The Purchase Schedule references the number, type, validity period, term, and pricing of Certificates, and number of domains.

2.3. Taxes. This Agreement is entered into, and all of the services are performed and provided, entirely within the United States of America. All fees for services are exclusive of any taxes however imposed, e.g. sales tax, income tax, GST, or VAT. Customer is solely responsible for calculating and paying all tax obligations resulting from Customer's acceptance of this Agreement, including sales tax, income tax, GST, or VAT but excluding all taxes based on DigiCert's income. Customer may not withhold or offset any amount owed to DigiCert for any reason. If a withholding or deduction is required by law, then Customer will pay an additional amount that is equal to the amount withheld or deducted, causing DigiCert to receive a net amount from Customer that is equal to the amount DigiCert would receive if a withholding or deduction was not required.

3. Intellectual Property Rights.

3.1. DigiCert Intellectual Property Rights. DigiCert retains, and Customer will not obtain or claim, any title, interest, or ownership rights in the Certificates, API, and Account, including all software associated with the Account and API and any techniques and ideas embedded therein, all copies or derivative works of the Certificates or software provided by DigiCert, regardless of who produced, requested, or suggested the copy or derivative work, all documentation and marketing material provided by DigiCert to Customer, and all of DigiCert's copyrights, patent rights, trade secret rights and other proprietary rights.

3.2. Restrictions. Each party will protect the other party's intellectual property, good will, and reputation when accessing or using the other party's services or products. DigiCert may terminate this Agreement or restrict access to the Account if DigiCert reasonably believes that Customer is using the Account or Certificates to post or make accessible any material that infringes DigiCert's or any third party's rights. Customer will not use any marketing material or documentation that refers to DigiCert or its products or services without receiving written prior approval from DigiCert, except as outlined in section 3.3.

3.3. Trademark Usage. Either party may use the trademarks of the other to indicate that Customer is receiving DigiCert's services provided that such use would not foreseeably diminish or damage the other party's rights in the trademark, create a misrepresentation of the parties' relationship, or diminish or damage a party's reputation, including using a Certificate with a website that could be considered associated with crime, defamation, or copyright infringement. Neither party may register or claim any right in the other party's trademarks.

4. Confidentiality.

4.1. Definition. **"Confidential Information"** means any information, documentation, system, or process disclosed by a party or a party's affiliate that is (i) designated as confidential (or a similar designation) at the time of disclosure, (ii) disclosed in circumstances of confidence, or (iii) understood by the parties, exercising reasonable business judgment, to be confidential. Confidential Information does not include information that (a) was lawfully known or received by the receiving party prior to disclosure, (b) is or becomes part of the public domain other than as a result of a breach of this Agreement, (c) was disclosed to the receiving party by a third party, provided such third party, or any other party from whom such third party receives such information, is not in breach of any confidentiality obligation in respect to such information, or (d) is independently developed by the receiving party as evidenced by independent written materials.

4.2. Obligations. Each party will keep confidential all Confidential Information it receives from the other party or its affiliates. Each party will use disclosed Confidential Information only for the purpose of exercising its rights and fulfilling its obligations under this Agreement and will protect all Confidential Information against disclosure using a reasonable degree of care. Each party may disclose Confidential Information to its contractors if the contractor is contractually obligated to confidentially provisions that are at least as protective as those contained herein. If a receiving party is compelled by law to disclose Confidential Information of the disclosing party, the receiving party will use reasonable efforts to (i) seek confidential treatment for the Confidential Information, and (ii) send sufficient prior notice to the other party to allow the other party to seek protective or other court orders.

4.3. Publication of Certificate. Customer consents to (i) DigiCert's public disclosure of information embedded in an issued Certificate and (ii) DigiCert's transfer of Customer's information to servers located inside the United States. This consent survives termination of this Agreement. DigiCert may rely on and use information provided by Customer for any purposes connected to the services, only if such use is in compliance with the DigiCert's Privacy Policy available at https://www.digicert.com/digicert-privacy-policy.htm and complies with the confidentiality obligations in Section 4.2.

5. Termination.

5.1. Term. This Agreement is effective upon Customer's acceptance and will remain in effect unless earlier terminated in accordance with this Agreement.

5.2. Termination for Convenience. Customer may terminate this Agreement for any reason upon 7 days' written notice if Customer has paid all fees due.

5.3. Other Termination. Either party may terminate this Agreement immediately if the other party (i) materially breaches this Agreement and fails to remedy the material breach within 7 days after receiving notice of the material breach, (ii) engages in illegal or fraudulent activity or an activity that could materially harm the terminating party's business, (iii) has a receiver, trustee, or liquidator appointed over substantially all of its assets, (iv) has an involuntary bankruptcy proceeding filed against it that is not dismissed within 30 days of filing, or (v) files a voluntary petition of bankruptcy or reorganization.

5.4. Events Upon Termination. If this Agreement is terminated under Section 5.3, DigiCert may revoke the Certificates issued under this Agreement. In the case of termination under any other circumstance, provided that Customer remits full payment for the Certificate prior to this Agreement's termination date, (i) any Certificate issued prior to termination will remain valid until the earlier of the expiration of the Certificate's validity period or the Certificate is revoked as permitted under the Certificate Terms of Use, and (ii) Customer may access and use the Account solely to manage existing Certificates. Upon termination: (a) Customer may continue to use unrevoked Certificates in accordance with the Certificate Terms of Use, (b) except as otherwise specified, all other rights and licenses granted herein terminate, (c) each party will immediately discontinue all representations or statements that could imply that a relationship exists between DigiCert and Customer, (d) each party will continue to comply with the confidentiality requirements in this Agreement, and (e) Customer will, within 30 days of termination, pay to DigiCert any fees, or part thereof, still owed as of the date of termination and destroy or deliver to DigiCert all sales manuals, price lists, literature and other materials relating to DigiCert.

5.5. Survival. The Certificate Terms of Use survive termination of this Agreement until all Certificates issued expire or are revoked. In addition, the obligations and representations of the parties under Section 3.1, Section 3.2, Section 4 (Confidentiality), Section 5 (Termination), Section 6 (Disclaimers of Warranties, Limitation of Liability, and Indemnification), and Section 7 (Miscellaneous) survive termination of this Agreement. All amounts owed by Customer for services and products issued prior to termination remain owed after termination of this Agreement.

6. Disclaimer of Warranties, Limitation of Liability, and Indemnification.

6.1. Warranty Disclaimers. THE ACCOUNT, CERTIFICATES, AND ANY RELATED SOFTWARE ARE PROVIDED "AS IS" AND "AS AVAILABLE." TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET CUSTOMER'S EXPECTATIONS OR THAT ACCESS TO THE ACCOUNT WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

6.2. Limitation of Liability. This Agreement does not limit a party's liability for (i) death or personal injury resulting from the negligence of a party or (ii) fraud or fraudulent statements made by a party. TO THE FULL EXTENT PERMITTED BY APPLICABLE LAW AND NOTWITHSTANDING ANY FAILURE OF ESSENTIAL PURPOSE OF ANY LIMITED REMEDY OR LIMITATION OF LIABILITY: (A) DIGICERT AND ITS AFFILIATES, SUBSIDIARIES, OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, PARTNERS AND LICENSORS (THE "DIGICERT

ENTITIES") WILL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, OR PUNITIVE DAMAGES (INCLUDING ANY DAMAGES ARISING FROM LOSS OF USE, LOSS OF DATA, LOST PROFITS, BUSINESS INTERRUPTION, OR COSTS OF PROCURING SUBSTITUTE SOFTWARE OR SERVICES) ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SUBJECT MATTER HEREOF; AND (B) DIGICERT ENTITIES' TOTAL CUMULATIVE LIABILITY ARISING OUT OF OR RELATING TO THIS AGREEMENT OR THE SUBJECT MATTER HEREOF WILL NOT EXCEED THE AMOUNTS PAID BY CUSTOMER TO DIGICERT IN THE TWELVE (12) MONTHS PRIOR TO THE EVENT GIVING RISE TO SUCH LIABILITY, IN EACH OF THE FOREGOING CASES (A) AND (B), REGARDLESS OF WHETHER SUCH LIABILITY ARISES FROM CONTRACT, INDEMNIFICATION, WARRANTY, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHERWISE, AND REGARDLESS OF WHETHER DIGICERT HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH LOSS OR DAMAGE.

6.3. Indemnity. Customer will indemnify, defend and hold harmless DigiCert and DigiCert's employees, officers, directors, shareholders, affiliates, and assigns against all third party claims and all related liabilities, damages, and costs, including reasonable attorneys' fees, arising from (i) Customer's breach of this Agreement, (ii) Customer's failure to protect the authentication mechanisms used to secure the Account, (iii) an allegation that personal injury or property damage caused by the fault or negligence of Customer, (iv) Customer's failure to disclose a material fact related to the use or issuance of the Account or Certificate, or (v) an allegation that the Customer, or an agent of Customer, used DigiCert's products or services to infringe on the rights of a third party.

6.4. Indemnity Obligations. An entity seeking indemnification under this Agreement ("**Indemnified Party**") must notify Customer promptly of any event requiring indemnification. However, an Indemnified Party's failure to notify will not relieve Customer from its indemnification obligations, except to the extent that the failure to notify materially prejudices Customer. Customer may assume the defense of any proceeding requiring indemnification unless assuming the defense would result in potential conflicting interests as determined by the Indemnified Party in good faith. An Indemnified Party may, at Customer's expense, defend itself until Customer's counsel has initiated a defense of the Indemnified Party. Even after Customer assumes the defense, the Indemnified Party may participate in any proceeding using counsel of its own choice and at its own expense. Customer may not settle any proceeding related to this Agreement unless the settlement also includes an unconditional release of liability for all Indemnified Parties. Customer's indemnification obligations are not the sole remedy for Customer's breach of this Agreement and are in addition to any other remedies available.

6.5. Extent. The limitations and obligations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this Agreement were breached or proven ineffective.

7. Miscellaneous.

7.1. Force Majeure. Except for Customer's payment obligations, neither party is liable for any failure or delay in performing its obligations under this Agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonable control. Customer acknowledges that the Account and Certificates are subject to the operation and telecommunication infrastructures of the Internet and the operation of Customer's Internet connection services, all of which are beyond DigiCert's control.

7.2. Entire Agreement. This Agreement, along with all documents referred to herein, including the Purchase Schedule, constitute the entire agreement between the parties with respect to the subject matter, superseding all other prior agreements that might exist. All DigiCert products and services are provided only upon the terms and conditions of this Agreement, and this Agreement prevails over any conflicting, additional, or different terms and conditions proposed by Customer. Except as otherwise allowed herein, neither party may amend this Agreement unless the amendment is both in writing and signed by the parties. In the event of an inconsistency between documents, the following order of precedence will apply: (1) Certificate Services Agreement, (2) Certificate Terms of Use, (3) Purchase Schedule.

7.3. Amendment. DigiCert may amend (i) this Certificate Services Agreement, (ii) the Certification Practice Statement ("**CPS**"), available at https://www.digicert.com/ssl-cps-repository.htm, (iii) the Privacy Policy, and (iv) the Certificate Terms of Use at any time and will give notice of such changes. In the event an amendment materially and adversely affects Customer's rights herein, Customer will have the right, as its sole remedy, to terminate this Agreement within 30 days of DigiCert's notice of such amendment by providing written notice. Customer's continued use of the Account constitutes Customer's acceptance of the amendment.

7.4. Waiver. A party's failure to enforce or delay in enforcing a provision of this Agreement does not waive the party's right to enforce the same provision later or the party's right to enforce any other provision of this Agreement. A waiver is only effective if in writing and signed by the party benefiting from the waived provision.

7.5. Assignment. Customer may not assign any of its rights or obligations under this Agreement without the prior written consent of DigiCert. DigiCert may assign its rights and obligations without Customer's consent.

7.6. Relationship. DigiCert and Customer are independent contractors and not agents or employees of each other. Neither party has the power to bind or obligate the other. Each party is responsible for its own expenses and employees.

7.7. Notices**.** DigiCert will send notices of termination or breach of this Agreement to Customer by first class mail to the address listed in the Account, which notices are effective upon receipt. DigiCert will send all other notices by posting the notice in the Account or by email via the email address of Customer's administrator (and/or other alternate email address associated with Customer's Account if provided), or by regular mail. All such notices are effective when posted in the Account or when sent. It is Customer's responsibility to keep its email address current. Customer will be deemed to have received any email sent to the email address then associated with Customer's Account when DigiCert sends the email, regardless of whether Customer receives the email. Customer will send DigiCert notices in writing by postal mail that is addressed to DigiCert, Inc., Attn: General Counsel, 2801 North Thanksgiving Way, Suite 500, Lehi, Utah 84043. Notices from Customer are effective upon receipt.

7.8. Governing Law and Jurisdiction. The laws of the state of Utah govern the interpretation, construction, and enforcement of this Agreement and all matters related to it, including tort claims, without regards to any conflict-of-law principles. The parties hereby submit to the exclusive jurisdiction of and venue in the state and federal courts located in Utah County, Utah.

7.9. Severability. The invalidity or unenforceability of any provision of this Agreement, as determined by a court or administrative body of competent jurisdiction, will not affect the validity or enforceability of the remainder of this Agreement, and the provision affected will be construed so as to be enforceable to the maximum extent permissible by law.

7.10. Rights of Third Parties*.* Except as stated in the Certificate Terms of Use, no third parties have any rights or remedies under this Agreement.

7.11. Interpretation**.** The definitive version of this Agreement is written in English. If this Agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls.

Copyright Notice and Takedown Procedure

DigiCert respects the intellectual property rights of others and follows the procedures established under the Digital Millennium Copyright Act (“DMCA”). The notice and counter notice procedures described below are provided exclusively for notifying DigiCert about infringing material under its control. The information disclosed in a notice or counter notice is not considered confidential information and is not subject to DigiCert’s privacy policy.If you, the complaining party, believe that your work is being used in a way that constitutes copyright infringement, please notify DigiCert’s copyright agent by sending a written communication by email to **copyrightagent@digicert.com** or by U.S. mail to:

DigiCert, Inc.
ATTN: Copyright Agent
2801 North Thanksgiving Way
Suite 500
Lehi, UT 84043
United States

A notice is only effective if it includes:

- A physical or electronic signature of a person authorized to act on behalf of the owner of an exclusive right that is allegedly infringed,
- Identification of the copyrighted work claimed to be infringed,
- A reasonably sufficient identification of the material claimed as infringing or that is the subject of infringing activity and that is to be removed or disabled,
- The complaining party’s contact information, such as an address, telephone number, and email address,
- A statement that the complaining party has a good-faith belief that use of the claimed infringing material is not authorized by the copyright owner, its agent, or the law, and
- A statement that the information in the notification is accurate and that the complaining party is authorized to act on behalf of the owner of an exclusive right that is allegedly infringed.

After receiving a notice of infringement, DigiCert will review the complaint and take appropriate measures, including removing or disabling access to material that is alleged as infringing. When possible, DigiCert will forward a copy of the notification to the party that is allegedly infringing the copyrighted material (“Alleged Infringer”). DigiCert will also notify the Alleged Infringer of any action taken as a result of the notice.The Alleged Infringer may provide a written counter notice to DigiCert’s copyright agent. An effective counter notice must include:

- An electronic or physical signature of the Alleged Infringer,
- Identification of the material that DigiCert removed or to which access was disabled and the location from which the removed material was removed or the location where access was disabled,

- A statement that the Alleged Infringer believes, in good faith and under the penalty of perjury, that the material was removed or disabled as a result of a mistake or misidentification of infringing material,
- The Alleged Infringer's name, address, and telephone number,
- The Alleged Infringer's consent to the jurisdiction of Federal District Court for the judicial district in which the Alleged Infringer is located (or Utah if the Alleged Infringer's address is outside of the United States) and a statement that the Alleged Infringer will accept service of process from the person or an agent of the person who provided notice of the infringement.

DigiCert will provide the complaining party a copy of the counter notice and will give the complaining party ten days notice before replacing or re-enabling access to removed material. DigiCert will replace any removed material or cease disabling access to the material between ten and fourteen business days after the counter notice is forwarded to the complaining party, provided that DigiCert has not received notice that that the complaining party has initiated a formal legal proceeding to restrain the Alleged Infringer from engaging in infringing activity that is related to the material under DigiCert's control

DigiCert Certificate Terms of Use

These terms apply to each digital certificate (**“Certificate”**) issued by DigiCert, Inc., a Utah corporation (**“DigiCert”**) to an entity or person (**“Customer”**), as identified in the Account or issued Certificates. By accepting an agreement that incorporates these terms, (such agreement, together with these terms, collectively, the **“Agreement”**), the signer is entering Customer into a legally valid and enforceable agreement to obtain a form of digital identity for the Customer. The signer acknowledges that he/she has the authority to obtain the digital equivalent of a company stamp, seal, or officer’s signature to establish the authenticity of Customer’s website, and that Customer is responsible for all uses of the Certificate. By accepting an Agreement on behalf of Customer, the signer represents that he/she (i) is acting as an authorized representative of Customer, (ii) is expressly authorized by Customer to sign the Agreement and approve Certificate requests on Customer’s behalf, and (iii) has or will confirm Customer’s exclusive right to use the domain(s) to be included in any issued Certificates. Customer and DigiCert agree as follows:

1.
   1.
      1. **Requests.** Customer may request SSL Certificates only for domain names registered to Customer, an affiliate of Customer, or an entity that expressly authorizes DigiCert to allow Customer to obtain and manage Certificates for the domain name. DigiCert may limit the number of domain names that Customer may include in a single Certificate in its sole discretion.
      2. **Verification.** After receiving a request for a Certificate through the Account, DigiCert will review the request and attempt to verify the relevant information in accordance with the DigiCert CPS and industry standards. **“Account”** means a DigiCert system account and API. Verification is subject to DigiCert’s sole discretion, and DigiCert may refuse to issue a Certificate for any reason. DigiCert will notify Customer if a Certificate request is refused but DigiCert is not required to provide a reason for the refusal. **“Certificate Practices Statement”** or **“CPS”** means DigiCert’s written statements of the policies and practices used to operate its PKI . DigiCert’s CPS documents are available at https://digicert.com/legal-repository.
      3. **Certificate Life Cycle.** The lifecycle of an issued Certificate depends on the selection made by Customer when ordering the Certificate, the requirements in the CPS, and the intended use of the Certificate. DigiCert may modify Certificate lifecycles for unissued Certificates as necessary to comply with requirements of (i) the Agreement, (ii) industry standards, (iii) DigiCert’s auditors, or (iv) an Application Software Vendor. Customer agrees to cease using a Certificate and its related Private Key after the Certificate’s expiration date. **“Application Software Vendors”** means an entity that displays or uses Certificates in connection with a distributed root store in which DigiCert participates or will participate.

4. **Issuance.** If verification is completed to DigiCert's satisfaction, DigiCert will issue and deliver the requested Certificate to Customer. DigiCert may deliver the Certificate using any reasonable means of delivery. Typically, DigiCert will deliver Certificates via email to an address specified by Customer as an electronic download in the Account or in response to an API call made by Customer. Certificates are issued from a DigiCert root or intermediate Certificate selected by DigiCert. DigiCert may change which root or intermediate certificate is used to issue Certificates at any time and without notice to Customer. Customer will abide by all applicable laws, regulations and industry standards when ordering and using Certificates, including United States export laws. Customer acknowledges that the Certificates are not available in countries restricted by the Office of Foreign Assets Control.
5. **Certificate License.** Effective immediately after delivery and continuing until the Certificate expires or is revoked, Customer may use, for the benefit of the Certificate's subject, each issued Certificate and corresponding Key Set for the purposes described in the CPS, in accordance with all applicable laws, regulations, industry standards, and with the terms herein. **"Key Set"** means a set of two or more mathematically related keys, referred to as Private Keys or key shares along with a Public Key, wherein (i) the Public Key can encrypt a message which only the Private Key(s) can decrypt, and (ii) even knowing the Public Key, it is computationally infeasible to discover the Private Key(s). Customer will promptly inform DigiCert if it becomes aware of any misuse of a Certificate, Private Key, or the Account. Customer is responsible for obtaining and maintaining any authorization or license necessary to order, use, and distribute a Certificate to end users and systems, including any license required under United States' export laws.
6. **Certificate Transparency.** To ensure Certificates function properly throughout their lifecycle, DigiCert may log SSL Certificates with a public certificate transparency database. Because this will become a requirement for Certificate functionality, Customer cannot opt out of this process. Log server information is publicly accessible. Once submitted, information cannot be removed from a log server.
7. **Client Certificates.** **"Client Certificate"** means a Certificate that contains any extendedKeyUsage other than codeSigning, timestamping or serverAuthentication. The Certificate uses are varied and are defined by the Client Certificate profile. Some of the possible uses defined in a Client Certificate profile may include, digital signature, email encryption, and cryptographic authentication. If Customer wishes to request Client Certificates, Customer must (i) confirm the identity and affiliation of the requester using appropriate internal documentation as prescribed the CPS and (ii) confirm that the information provided and representations related to or incorporated in any Client Certificate are true, complete, and accurate in all material respects.

8. **Key Sets.** A **“Private Key”** means the key that is kept secret by Customer that is used to create digital signatures and/or decrypt electronic records or files that were encrypted with the corresponding Public Key. A **“Public Key”** means Customer’s publicly-disclosed key that is contained in Customer’s Certificate and corresponds to the secret Private Key that Customer uses. Customer must (i) generate Key Sets using trustworthy systems, (ii) use Key Sets that are at least the equivalent of RSA 2048 bit keys, and (iii) keep all Private Keys confidential. Customer is solely responsible for any failure to protect its Private Keys. Customer represents that it will only generate and store Key Sets for Adobe Signing Certificates and EV Code Signing Certificates on a FIPS 140-2 Level 2 device. All other Certificate types may be stored on secure software or hardware systems.
9. **Management.** DigiCert will generally issue, manage, renew, and revoke a Certificate in accordance with any instructions submitted by Customer through the Account and may rely on such instructions as accurate. Customer will provide accurate and complete information when communicating with DigiCert and will notify DigiCert within 5 business days if any information relating to the Account changes. Customer will review and verify the Certificate data prior to using the Certificate for accuracy. Certificates are considered accepted 30 days after the Certificate’s issuance, or earlier upon use of the Certificate when evidence exists that the Customer used the Certificate. Although DigiCert may send a reminder about expiring Certificates DigiCert is under no obligation to do so and Customer is solely responsible for ensuring Certificates are renewed prior to expiration.
10. **Security and Use of Key Sets.** Customer will securely generate and protect the Key Sets associated with a Certificate and take all steps necessary to prevent the compromise, loss, or unauthorized use of a Private Key associated with a Certificate. Customer will use passwords that are randomly generated with at least 16 characters containing uppercase letters, lowercase letters, numbers, and symbols to transport Private Keys. To minimize internal risk of Private Key compromise, Customer will only allow employees, agents, and contractors to access or use Private Keys if the employee, agent, or contractor has undergone a background check by Customer (to the extent allowed by law) and has training or experience in PKI and other information security fields. Customer will notify DigiCert, request revocation of a Certificate and its associated Private Key, cease using such Certificate and its associated Private Key, and remove the Certificate from all devices where it is installed if (i) any information in the Certificate is or becomes incorrect or inaccurate, (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the Public included in the Certificate. For code signing Certificates Customer will promptly cease using a Certificate and its associated Private Key and promptly request revocation of the Certificate if Customer believes that (a) any information in the Certificate

is, or becomes, incorrect or inaccurate, (b) the Private Key associated with the Public Key contained in the Certificate was misused or compromised, or (c) there is evidence that the Certificate was used to sign Suspect Code. **"Suspect Code"** means code that contains malicious functionality or serious vulnerabilities, including spyware, malware and other code that installs without the user's consent and/or resists its own removal, and code that can be exploited in ways not intended by its designers to compromise the trustworthiness of the platforms on which it executes. Customer will respond to DigiCert's instructions concerning Key Set compromise or Certificate misuse within 7 days. Customer will promptly cease using the Key Set corresponding to a Certificate upon the earlier of (I) revocation of the Certificate and (II) the date when the allowed usage period for the Key Set expires. After revocation, Customer must cease using the Certificate.

11. **Defective Certificates.** Customer's sole remedy for a defect in a Certificate is to require DigiCert to use commercially reasonable efforts to cure the defect after receiving notice from Customer. DigiCert is not obligated to correct a defect if (i) Customer misused, damaged, or modified the Certificate, (ii) Customer did not promptly report the defect to DigiCert, or (iii) Customer has breached any provision of the Agreement.
12. **Relying Party Warranty.** Customer acknowledges that the Relying Party Warranty is only for the benefit of Relying Parties. Customer does not have rights under the warranty, including any right to enforce the terms of the warranty or make a claim under the warranty. **"Relying Party"** means an entity other than Customer that acts in reliance on a Certificate or a digital signature. An Application Software Vendor is not a Relying Party when the software distributed by the Application Software Vendor merely displays information regarding a Certificate or facilitates the use of the Certificate or digital signature. **"Relying Party Warranty"** means a warranty offered to a Relying Party that meets the conditions found in the Relying Party Warranty Agreement posted on DigiCert's website at /docs/agreements/DigiCert_RPA.pdf.
13. **Representations.** For each requested Certificate, Customer represents to DigiCert that:
    a. Customer has the right to use or is the lawful owner of (i) any domain name(s) specified in the Certificate and (ii) any common name or organization name specified in the Certificate
    b. the individual accepting the Agreement is expressly authorized by Customer to enter into an Agreement on behalf of Customer,
    c. Customer will use the Certificate only for authorized and legal purposes, including not using the Certificate to sign Suspect Code and to use the Certificate and Private Key solely in compliance with all applicable laws and solely in accordance with the Certificate purpose, the CPS, any applicable certificate policy, and the Agreement,
    d. Customer has read, understands, and agrees to the CPS, and

e. the organization included in the Certificate and the registered domain name holder is aware of and approves of each Certificate request.

14. **Restrictions.** Customer will only use a TLS/SSL Certificate on the servers accessible at the domain names listed in the issued Certificate. Additionally, Customer will not:

    a. modify, sublicense, or create a derivative work of any Certificate (except as required to use the Certificate for its intended purpose) or Private Key,

    b. upload or distribute any files or software that may damage the operation of another’s computer,

    c. make representations about or use a Certificate except as allowed in the CPS,

    d. impersonate or misrepresent Customer’s affiliation with any entity,

    e. use the Certificate or any related software (such as the Account) in a manner that could reasonably result in a civil or criminal action being taken against Customer or DigiCert,

    f. use the Certificate or any related software to breach the confidence of a third party or to send or receive unsolicited bulk correspondence,

    g. use code signing Certificates to sign Suspect Code,

    h. apply for a code signing Certificate if the Public Key in the Certificate is or will be used with a non-code signing Certificate

    i. interfere with the proper functioning of the DigiCert website or with any transactions conducted through the DigiCert website,

    j. attempt to use a Certificate to issue other Certificates, or

    k. intentionally create a Private Key that is substantially similar to a DigiCert or third party Private Key.

15. **Certificate Revocation.** DigiCert may revoke a Certificate without notice for the reasons stated in the CPS, including if DigiCert reasonably believes that:

    a. Customer requested revocation of the Certificate or did not authorize the issuance of the Certificate,

    b. Customer has breached the Agreement or an obligation it has under the CPS,

    c. any provision of an agreement with Customer containing a representation or obligation related to the issuance, use, management, or revocation of the Certificate terminates or is held invalid,

    d. Customer is added to a government prohibited person or entity list or is operating from a prohibited destination under the laws of the United States,

    e. the Certificate contains inaccurate or misleading information,

    f. the Certificate was used without authorization, outside of its intended purpose or used to sign Suspect Code,

    g. the Private Key associated with the Certificate was disclosed or compromised,

    h. the Certificate was (i) misused, (ii) used or issued contrary to law, the CPS, or industry standards, or (iii) used, directly or indirectly, for illegal or fraudulent purposes, such as phishing attacks, fraud, or the distribution of malware or other illegal or fraudulent purposes,

i. industry standards or DigiCert's CPS require Certificate revocation, or revocation is necessary to protect the rights, confidential information, operations, or reputation of DigiCert or a third party.

16. **Sharing of Information.** Customer acknowledges and accepts that if (i) the Certificate or Customer is identified as a source of Suspect Code, (ii) the authority to request the Certificate cannot be verified, or (iii) the Certificate is revoked for reasons other than Customer request (e.g. as a result of private key compromise, discovery of malware, etc.), DigiCert is authorized to share information about Customer, the signed application, the Certificate, and the surrounding circumstances with other certification authorities or industry groups, including the CA/Browser Forum.
17. **Industry Standards.** Both parties will comply with all industry and privacy standards that apply to the Certificates. If a law or industry standard changes and that change affects the Certificates or other services provided under the Agreement, then DigiCert may amend the Agreement to the extent necessary to comply with the change.
18. **Equipment.** Customer is responsible, at Customer's expense, for (i) all computers, telecommunication equipment, software, access to the Internet, and communications networks (if any) required to use the Certificates and related DigiCert software or services, and (ii) Customer's conduct and its website maintenance, operation, development, and content.
19. **Certificate Beneficiaries.** Relying Parties and Application Software Vendors are express third party beneficiaries of Customer's obligations and representations related to the use or issuance of a Certificate. The Relying Parties and Application Software Vendors are not express third party beneficiaries with respect to any DigiCert software.

Last updated January 30, 2017

DigiCert Cookie Policy

To maintain transparency and inform users about how DigiCert gathers and uses visitor information, we have compiled a list of cookies DigiCert uses to assist customers and improve DigiCert's services.

What Are Cookies?

Cookies are small text files placed on a computer when visiting a website. Cookies are used to provide session information and services, save information between multiple visits to a site, and provide the website operator information about a user's website experience. DigiCert uses cookies for the following purposes:

Session Cookies

Session tracking cookies provide a consistent experience between related web pages. These cookies last for a specified amount of time, typically the duration that the user is using the website. Web browsers delete session cookies when the browser is closed.

PHP Session ID

DigiCert's PHP Session Cookies maintain user settings and information, such as the preferred website language setting and account login status. These cookies keep the user logged in while visiting various pages across the DigiCert site.

Customer Experience Cookies

Customer experience cookies provide DigiCert anonymous information about a customer's use of the DigiCert website. Cookies are not used to gather personally identifiable information.

These cookies are primarily used to optimize a user's browsing experience, provide targeting advertising, and improve DigiCert's website. Some of these are third-party cookies that are provided to users when visiting the DigiCert website. Third party cookies include:

Google and Adobe Analytics

Google and Adobe Analytics are web analysis tools that use cookies to track and compile website information. For example, Google and Adobe Analytics may use cookies to collect information about the number of website visitors DigiCert receives on a daily basis, how new customers found the DigiCert website, and the value DigiCert's website provides. DigiCert uses this information to improve its services and website. The information collected by Google and Adobe Analytics is anonymous and collects only general information and trends.

Optimizely

Optimizely is a website testing tool that uses cookies to serve unique test versions to a site visitor. For example, a web visitor may view a page that we are trying to improve, and will be shown a longer format page, whereas another visitor would be shown a shorter format page. Optimizely enables DigiCert to test different versions of pages, determine which version site visitors prefer, and use that data to improve usability of our website. The information collected by Optimizely is anonymous and collects only general data for testing analysis.

Google AdWords Remarketing

Google AdWords is an advertising tool that uses cookies to help businesses reach potential customers across the web through tailored marketing services. These cookies allow a business to target their marketing efforts towards specific customers by excluding current customers from advertising campaigns specific to non-customers, offering special promotions and discounts to existing customers, and providing similar customized marketing efforts.

Marketo

Marketo, a marketing automation solution, uses cookies to provide information on how a user interacts with DigiCert's website and emails. Marketo provides valuable information on a user's visit to high-interest web pages, completion of web forms, and interaction with both marketing and sales emails. These cookies allow DigiCert to refine our marketing efforts and provide more specific information to users.

Social Media

These cookies allow users to share pages and articles on social media sites while pulling information from the user's social media profile.

Removing and Disabling Tracking Cookies

To learn more about how third-party cookies collect and use information, please see Google's Advertising Privacy FAQ, and Marketo's Email Use and Anti-Spam Policy.

Removing Cookies

Most browsers allow users to remove undesired cookies. In Chrome, navigate to the “History” menu and select “Clear all browsing data…” In Internet Explorer, select “Internet Options” and “Delete…” under the Browsing History section. In Firefox, select “Clear recent history…” under the “History” menu. In Safari, choose “Reset Safari…” under the general settings menu. Most browsers also permit users to remove individual cookies.

Removing previously collected cookies will reset all website information. This includes removing the settings that exclude existing customers from receiving advertisements meant for non-customers and vice-versa.

Disabling Cookies

Most browsers allow users to disable cookies. This option is usually available in the browser’s privacy settings where users can choose to disable cookies entirely or reject cookies from specific providers.

Disabling cookies may cause some websites and shopping carts to stop functioning properly and will lead to less personalized and targeted advertising. Disabling cookies may also reset all website information between each visit, causing websites to treat returning customers as new visitors

DigiCert Legal Repository

This page contains information relating to the use and issuance of certificates by DigiCert. For compatibility-related information, see our
DigiCert certificate compatibility page.

Current Legal Documentation

DigiCert Certificate Policy (CP)
For certificates issued on or after February 23, 2017

DigiCert Certification Practices Statement (CPS)
For certificates issued on or after February 23, 2017

DigiCert Certificate Services Agreement

DigiCert Certificate Terms of Use

DigiCert Website Terms of Use

DigiCert Privacy Policy

DigiCert Cookie Policy

DigiCert Copyright Notice and Takedown Procedure

DigiCert Trademark Usage Guidelines

DigiCert Relying Party Agreement and Limited Warranty
Notice: You must read this Relying Party Agreement before relying on a DigiCert-issued SSL certificate or Site Seal.

Archived CP/CPS Documentation

DigiCert Certificate Policy (CP)
For certificates issued on or after September 9, 2016 and before February 23, 2017

DigiCert Certification Practices Statement (CPS)
For certificates issued on or after September 9, 2016 and before February 23, 2017

DigiCert Certificate Policy (CP)
For certificates issued on or after July 1, 2015 and before September 9, 2016

DigiCert Certification Practices Statement (CPS)
For certificates issued on or after April 1, 2015 and before June 1, 2015

DigiCert Certificate Policy (CP)
For Certificates issued on or after April 1, 2015 and before June 1, 2015

DigiCert Certification Practices Statement (CPS)
For Certificates issued on or after April 1, 2015 and before June 1, 2015

DigiCert Certificate Policy (CP)
For certificates issued on or after October 7, 2014 and before April 1, 2015

DigiCert Certification Practices Statement (CPS)
For certificates issued on or after October 7, 2014 and before April 1, 2015

DigiCert Certificate Policy (CP)
For certificates issued on or after May 14, 2014 and before October 7, 2014

DigiCert Certification Practices Statement (CPS)
For certificates issued on or after May 14, 2014 and before October 7, 2014

DigiCert Certificate Policy (CP)
For certificates issued on or after May 2, 2013 and before May 14, 2014

DigiCert Certificate Practices Statement (CPS)
For certificates issued on or after May 2, 2013 and before May 14, 2014

WebTrust Report

2017 Generic WebTrust

2017 EV SSL

2017 WebTrust Report

Privacy Policy Archive

DigiCert Privacy Policy Effective Date September 27, 2016-redlined
DigiCert Privacy Policy Effective Date August 10, 2017-redlined

DigiCert Privacy Policy

Effective Date of Privacy Policy

Changes will become effective August 10, 2017
Privacy Policy Archive

Introduction

DigiCert, Inc. ("DigiCert", "we" or "us") is committed to protecting the privacy of its customers and website visitors ("you"). As a result, DigiCert has developed this privacy policy to inform its website visitors and customers about how DigiCert collects, uses, shares and secures your personal information, as well as your choices regarding use, access and correction of your personal information. This privacy policy applies to www.digicert.com, a site owned and operated by DigiCert.

Non-Personal Information

DigiCert, like most website operators, uses cookies, web beacons and log files to automatically gather, analyze, and store non-personal information about website visitors. Non-personal information may include the visitor's IP address, browser type, ISP, referring page, operating system, date/time, and clickstream data. DigiCert uses third-party software to assist in collecting and analyzing this information. This information is used to improve DigiCert's service and enhance the experience of DigiCert's website visitors.

Technologies such as cookies, beacons, tags, and scripts are used by DigiCert and our third party service providers to analyze trends, administer the site, track users' movements around the site, and gather demographic information about our user base as a whole. We may receive reports based on the use of these technologies by these companies on an individual as well as aggregated basis. Visit our Online Cookies and Privacy page for a list of cookies used on the DigiCert website. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our website or service. To manage Flash cookies, please click here.

DigiCert uses a third party to either display advertising on our website or to manage our advertising on other sites. Our third party partner may use technologies such as cookies to gather information about your activities on our site and other sites in order to provide you advertising based upon your browsing activities and interests. If you wish to not have information used for the purpose of serving you interest-based ads, you may opt-out by clicking here (or if located in the European Union click here). Please note this does not opt you out of being served ads. You will continue to receive generic ads.

Personal Information

In order to provide quality communication, DigiCert collects information such as the name, organization, and email address of website visitors who voluntarily submit that information to download software or to submit sales or technical support questions. We also collect information required to issue certificates (as specified in our Certification Practices Statement on the Legal Repository) when you buy certificates from our site. This information is voluntarily submitted by the customer or is obtained from third party databases during the validation process.

Regardless of the source, DigiCert protects personal information as confidential information except where the information is embedded in an issued digital certificate. This information is necessary for the digital certificate's operation and is considered public information.

When performing validation, DigiCert uses third party sources to confirm or supplement customer information. We may receive information about you from other sources, including third parties from whom we have purchased access to certain data, and combine this data with information we already have about you. We may confirm or supplement, for instance, address, email and company name for validation and verification purposes.

Accessing and Updating Personal Information

Generally, a customer can review, delete inaccuracies, and update personal information through its DigiCert account interface by clicking edit under the Account Profile tab. Upon request DigiCert will provide you with information about whether we hold any of your personal information. You may also access, correct, or request deletion of your personal information by sending an email to privacy@digicert.com or by mailing DigiCert at the address listed in this policy. Emailed and mailed requests are subject to DigiCert's satisfaction regarding the authenticity of the request. We will respond to your request within a reasonable timeframe.

DigiCert retains information about customers while the customer's account is active, while a certificate remains unexpired, and in accordance with industry standards. A customer may request account cancellation or request that DigiCert no longer provide services by emailing privacy@digicert.com. DigiCert may retain certain customer information after receiving a request to cancel services or disable an account, as necessary to comply with industry standards and legal obligations, to resolve disputes, and to enforce customer agreements.

Personal information embedded in a digital certificate cannot be directly edited. Customers wishing to update personal information in a digital certificate must submit a change request through the customer account. DigiCert may require that the updated information be verified for accuracy prior to accepting the change request. In addition, even if information is updated in DigiCert's databases, the information will generally not be updated in the issued digital certificate. If information embedded in a digital certificate needs updating, DigiCert may require revocation of the digital certificate.

Use of Information

Products and Services

DigiCert may use personal information to market, sell and provide its products and services, send an order confirmation, respond to customer service requests, and fulfill your order, including using the information to verify the identity of the customer or to contact the customer in order to discuss support, renewal, and the purchase of products and services.

As discussed further in the “Sharing With Third Parties” section below, DigiCert may allow its business partners to assist in providing requested products and services. All such DigiCert service providers are required to keep personal information confidential and are only allowed to use the information to the extent necessary to provide the requested products and services.

Live Chat Sales/Support

DigiCert utilizes a live chat tool for assisting our customers with sales questions and technical support needs; in addition to the customer’s name and email address (for purposes of communication), this tool collects information in accordance with the “Non-Personal Information” section above.

Emails

DigiCert may send out promotional emails (such as a newsletter) to individuals who provide personal information and have not opted-out of DigiCert’s mailing list. These emails may include beacons that communicate information about the email back to DigiCert. This communication allows DigiCert to gauge the effectiveness of its advertising and marketing campaigns. Recipients may opt-out of receiving promotional communication from DigiCert by following the unsubscribe instructions provided in each promotional email or by emailing privacy@digicert.com.

DigiCert also sends out advisory emails. Advisory emails are related to the primary purpose for which the information was collected and are used to respond to inquiries, provide support and validation services, provide upgrade information and security updates, and inform the customer about ordered products and services. Because advisory emails contain essential information related to the use and security of DigiCert’s products and services, customers may not unsubscribe from advisory emails.

DigiCert may use third parties, with which it has a confidentiality agreement, to send promotional or advisory emails. However, DigiCert restricts its partners from sending spam associated with DigiCert’s site, brand, or products. A customer receiving an unsolicited email related to DigiCert’s products and services should forward the entire message and headers to privacy@digicert.com.

Sharing With Third Parties

We will share your personal information with third parties only in the ways that are described in this privacy policy.

DigiCert never sells personal information to third parties. We may share your information with third parties who provide services on our behalf to help with our business activities. These companies are authorized to use your personal information only as necessary to provide these services to us.

DigiCert uses a third party to process credit card payments and may provide credit card numbers and identifying financial data directly to the third party credit card processor. These companies do not retain, share, store, or use personally identifiable information for any other purposes. DigiCert does not permanently store any provided credit card information.

DigiCert also uses a third party to provide its chat-based support. The support software allows users to input information, including an email address, to request support and clarify their problem. The software provider does not share inputted information with anyone other than DigiCert.

DigiCert may disclose information when required by law or when disclosure is necessary to protect DigiCert's rights and/or comply with a judicial proceeding, court order, bankruptcy proceedings, or similar legal process.

DigiCert will notify all interested parties if DigiCert is involved in a merger, acquisition, or sale of all or a portion of its assets that materially affects how DigiCert collects and stores personal information. Typically, this notice will be by email and/or a prominent notice on our website.

Referrals

If you choose to use our referral service to tell a friend about our site, we will ask you for your friend's name and email address. We will automatically send your friend a one-time email inviting him or her to visit the site. DigiCert collects this information for the sole purpose of sending this one-time email and tracking success of the referral program.

Your friend may contact us at privacy@digicert.com to request that we remove this information from our database.

Testimonials

With prior permission from the customer, DigiCert displays personal testimonials of satisfied customers on its website in addition to other endorsements. Customers wishing to update or delete a testimonial may contact DigiCert at privacy@digicert.com.

Blogs

Our website offers publicly accessible blogs or community forums. You should be aware that any information you provide in these areas may be read, collected, and used by others who access them.

Our blog is also managed by a third party application that may require you to register to post a comment. We do not have access or control of the information posted to the blog. You will need to contact or login to the third party application if you want the personal information that was posted to the comments section removed. To learn how the third party application uses your information, please review their privacy policy.

Social Media Widgets

The DigiCert website includes social media features, such as a Facebook “Like” button and widgets, as well as share buttons or interactive mini-programs. These features may collect the user”s IP address, the pages visited on DigiCert’s site, and may set a cookie to enable the feature to function properly. Social media features are either hosted by a third party or hosted directly on DigiCert’s site. Interactions with these features are governed by the privacy policy of the corresponding social media company.

Security

The security of your personal information is of the utmost importance to DigiCert. DigiCert only transmits personal information, including sensitive information (such as credit cards), using secure sockets layer technology (SSL). To learn more about SSL, follow this link https://www.digicert.com/ssl/.

Unfortunately, no method of transmission over the Internet or electronic storage is 100% secure. While DigiCert strives to use commercially acceptable standards to protect personal information, DigiCert cannot guarantee absolute security. If you have any questions about the security of your personal information, please contact us at privacy@digicert.com.

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

DigiCert participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. We are committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on each Privacy Shield Framework, to the Framework’s applicable Principles. To learn more about the Privacy Shield Frameworks, and to view our certification, visit the U.S. Department of Commerce’s Privacy Shield List, here.

DigiCert is responsible for the processing of personal data it receives, under each Privacy Shield Framework, and subsequently transfers to a third party acting as an agent on its behalf. DigiCert complies with the Privacy Shield Principles for all onward transfers of personal data from the EU and Switzerland, including the onward transfer liability provisions.

With respect to personal data received or transferred pursuant to the Privacy Shield Frameworks, DigiCert is subject to the regulatory enforcement powers of the U.S. Federal Trade Commission. In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements.

If you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

Under certain conditions, more fully described on the Privacy Shield website here, you may be entitled to invoke binding arbitration when other dispute resolution procedures have been exhausted.

Applicability

This privacy policy does not apply to any downloadable software provided through DigiCert”s websites.

Third party sites may link to or from DigiCert websites. DigiCert is not responsible for the privacy practices or the content of those other websites. We encourage you to carefully read the privacy policies of those third party sites.

Changes to This Privacy Policy

DigiCert may modify its privacy policy and related practices at any time. DigiCert will notify interested parties of material changes by either posting a notice on its home page or by emailing affected individuals. Visitors and customers should check the DigiCert website regularly to be aware of changes. We may update this privacy policy to reflect changes to our information practices. If we make any material changes we will notify you by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices. Revisions to the privacy policy are effective 30 calendar days after being posted.

Contact

Please contact DigiCert with any questions or concerns about this privacy policy or our data collection practices:

By mail:

DigiCert, Inc.
2801 North Thanksgiving Way
Suite 500
Lehi, Utah 84043

By phone or fax:

Toll Free: 1-800-896-7973 (US & Canada)
Direct: 1-801-701-9600
Fax Toll Free: 1-866-842-0223 (US & Canada)
Fax Direct: 801-705-0481

By email:

privacy@digicert.com

For assistance with technical difficulties, including problems with accessing or using your customer account, please email support@digicert.com.

As noted above, if you have an unresolved privacy or data use concern that we have not addressed satisfactorily, please contact our U.S.-based third-party dispute resolution provider (free of charge) at https://feedback-form.truste.com/watchdog/request.

DigiCert Legal Repository

The DigiCert Legal Repository is available at: DigiCert Legal Repository

DigiCert Website Terms of Use

PLEASE READ THESE TERMS CAREFULLY BEFORE USING OR ACCESSING A DIGICERT WEBSITE OR ANY CONTENT OR MATERIAL MADE ACCESSIBLE THROUGH A DIGICERT WEBSITE (COLLECTIVELY, “THE WEBSITES”). BY USING OR ACCESSING A DIGICERT WEBSITE, YOU AGREE TO THE TERMS HEREIN. IF YOU DO NOT AGREE TO THESE TERMS, DO NOT ACCESS OR USE A DIGICERT WEBSITE. These terms apply only to the Website and are not the terms governing the purchase or use of DigiCert’s products or services.

The Websites are maintained by DigiCert, Inc. in order to provide information related to DigiCert’s products and services. DigiCert does not make any representations or warranties about the Websites and use of a Website is at your own risk. DigiCert may modify a Website or these terms without notice and in its sole discretion. All modifications are effective immediately after the change is made. Please review these terms each time you visit or access a Website to ensure that you are aware of any changes.

Licenses. You are granted a limited and revocable license to access the Website in accordance with these terms. You may not use a Website in any jurisdiction where its contents or use is restricted or prohibited by law. You may not use the Website for any purpose other than learning about DigiCert, ordering its products and services, or maintaining your customer account.

Information Collection. DigiCert collects and stores information in accordance with the privacy policy posted on the Website. You grant DigiCert an irrevocable and royalty-free license to use any information submitted to DigiCert through a Website. By submitting information to DigiCert, you represent that the information is accurate and that any use of the information will not violate the rights of a third party.

Proprietary Rights of DigiCert. The Websites consist of and contain proprietary rights owned by DigiCert and its licensors. Unless DigiCert gives you express written permission to the contrary, you may not copy or create derivative works of a Website for any reason, including utilizing framing technologies to enclose proprietary information. Any unauthorized use of DigiCert’s intellectual property on a third party website or for commercial purposes is expressly prohibited.

Proprietary Rights of Third Parties. DigiCert respects the intellectual property rights of others. Please contact legal@digicert.com if you believe that a DigiCert Website contains material that infringes on the rights of a third party.

Links. A Website may link to another website under the control of a third party. These links are provided for convenience only. DigiCert does not endorse, monitor, control or verify the contents of any third party website and is not liable for any content accessed through a link.

No Warranties. THE WEBSITES ARE PROVIDED ON AN "AS IS" AND "AS AVAILBLE" BASIS. DIGICERT DISCLAIMS ALL WARRANTIES AND REPRESENTATIONS RELATED TO THE WEBSITES, INCLUDING ANY WARRANTY ON THE ACCURACY OF INFORMATION PRESENTED TRHOUGH A WEBSITE AND ALL WARRANTIES RELATED TO NON-INFRINGEMENT, FITNESS FOR A PARTICULAR USE, AND NON-INFRINGEMENT. NOTHING ON A WEBSITE CONSTITUTES A WARRANTY ON DIGICERT'S PRODUCTS OR SERVICES.

Waiver of Liability. YOU WAIVE ALL LIABILITY OF DIGICERT RELATED TO THE WEBSITES, EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF LIABILITY. DigiCert is not responsible for any inaccurate content or information on a Website. DigiCert is also not responsible for problems or technical malfunctions of a Website or any equipment or software used to access a Website. DigiCert is not liable for any loss or damage related to the use of a DigiCert Website. The disclaimers and limitations on warranty herein apply to the maximum extent allowed by law.

Indemnity. YOU AGREE TO INDEMNIFY AND HOLD DIGICERT HARMLESS AGAINST ANY DAMAGES, FEES, AND EXPENSES (INCLUDING REASONABLE ATTORNEY FEES) RELATED TO A THIRD PARTY CLAIM WHERE SUCH CLAIM ARISES OUT OF YOUR USE OF A WEBSITE, INCLUDING YOUR USE OF A LINK ON A WEBSITE OR YOUR SUBMISSION OF INFORMATION THROUGH THE WEBSITE.

Governing Law. All Website-related disputes are governed by the laws of the state of Utah without regard to any conflict of law principles. You agree to personal jurisdiction by and exclusive venue in the state and federal courts in Utah County, Utah.

Other. These terms contain the entire agreement between you and DigiCert with respect to your use of the Websites. Any term held invalid by a competent court of law does not affect the validity and enforceability of the other terms herein.

Last updated 8/30/2010

Note: This Terms of Use Agreement is separate from other Agreements such as our Subscriber and CPS Agreements which is entered upon acceptance/submission of an order/application.

You can view the DigiCert Legal Repository by clicking here: DigiCert Legal Repository

To purchase a DigiCert SSL Certificate, click here.

DigiCert

Certificate Policy

DigiCert, Inc.
Version 4.11
February 23, 2017

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

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

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

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

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

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

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

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

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

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

1.2. DOCUMENT NAME AND IDENTIFICATION

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

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

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

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

Minimum Requirements for Code Signing	2.16.840.1.114412.3.1.1
Extended Validation Code Signing*	2.16.840.1.114412.3.2
Windows Kernel Driver Signing	2.16.840.1.114412.3.11
Adobe Signing Certificates	2.16.840.1.114412.3.21
Client Certificate OID arc	2.16.840.1.114412.4.
Level 1 Certificates – Personal	2.16.840.1.114412.4.1.1
Level 1 Certificates – Enterprise	2.16.840.1.114412.4.1.2
Level 2 Certificates	2.16.840.1.114412.4.2
Level 3 Certificates – US	2.16.840.1.114412.4.3.1
Level 3 Certificates – CBP	2.16.840.1.114412.4.3.2
Level 4 Certificates – US	2.16.840.1.114412.4.4.1
Level 4 Certificates – CBP	2.16.840.1.114412.4.4.2
PIV-I OID arc	2.16.840.1.114412.4.5
PIV-I Hardware - keys require activation by the PIV-I Cardholder (PIV Auth, Dig Sig and Key Management)	2.16.840.1.114412.4.5.1
PIV-I Card Authentication - keys do not require PIV-I Cardholder activation	2.16.840.1.114412.4.5.2
PIV-I Content Signing – use by PIV-I-compliant CMS	2.16.840.1.114412.4.5.3
Grid Certificates	2.16.840.1.114412.4.31 or 2.16.840.1.114412.31 (Grid-only arc)
IGTF-Comparable to Classic with Secured Infrastructure	2.16.840.1.114412.4.31.1 (Client w/ Public) or 2.16.840.1.114412.31.4.1.1 (Client Grid Only)
IGTF-Comparable to Member-Integrated Credential Services with Secured Infrastructure	2.16.840.1.114412.4.31.5
IGTF Grid Host - Public Trust	2.16.840.1.114412.1.31.1
Grid-Only Host Certificate	2.16.840.1.114412.31.1.1.1
Authentication-Only Certificates	2.16.840.1.114412.6
Legacy arc	2.16.840.1.114412.81
Test arc	2.16.840.1.114412.99

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

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

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

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

1.3. PKI PARTICIPANTS

1.3.1. DigiCert Policy Authority and Certification Authorities

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

1.3.2. Registration Authorities

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

1.3.3. Subscribers

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

1.3.4. Relying Parties

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

1.3.5. Other Participants

When issuing PIV-I cards, the Issuer CA shall make a Card Management Systems (CMS) responsible for managing smart card token content. The Issuer CA shall ensure that the CMS meets the requirements described herein. The Issuer CA shall not issue any Certificate to a CMS that includes a PIV-I Hardware or PIV-I Card Authentication policy OID. Other participants include Bridge CAs and CAs that cross-certify Issuer CAs to provide trust among other PKI communities.

1.4. CERTIFICATE USAGE

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

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

1.4.1. Appropriate Certificate Uses

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

1.4.2. Prohibited Certificate Uses

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

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

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

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

1.5.2. Contact Person

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

1.5.3. Person Determining CPS Suitability for the Policy

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

1.5.4. CP Approval Procedures

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

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

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

"Applicant" means an entity applying for a certificate.

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

"EV Guidelines" is defined in section 1.1.

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

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

"**PIV-I Profile**" means the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Ver. 1.1, Date: May 5 2015.

"Private Key" means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

"Public Key" means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

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

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

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

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

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

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

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

1.6.2. Acronyms

CA	Certificate Authority or Certification Authority
CBP	Commercial Best Practices
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCPA	DigiCert Policy Authority
DV	Domain Validated
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HSM	Hardware Security Module
IANA	Internet Assigned Numbers Authority
ICANN	Internet Corporation for Assigned Names and Numbers
IdM	Identity Management System
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
MICS	Member-Integrated Credential Service (IGTF)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OV	Organization Validated
PIN	Personal Identification Number (e.g. a secret access code)
PIV-I	Personal Identity Verification-Interoperable
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

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

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

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

2.2. PUBLICATION OF CERTIFICATION INFORMATION

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

2.3. TIME OR FREQUENCY OF PUBLICATION

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

2.4. ACCESS CONTROLS ON REPOSITORIES

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

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

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

For PIV-I Certificates:

1. Issuer CAs shall include both a non-null subject name and subject alternative name in Certificates.
2. Issuer CAs shall indicate the Subscriber's association with an Affiliated Organization as follows:

   PIV-I Hardware:

   For certificates with an Affiliated Organization:
   cn=Subscriber's full name, ou=Affiliated Organization Name,{Base DN}
   For certificates with no Affiliated Organization:
   cn=Subscriber's full name, ou=Unaffiliated, ou=Entity CA's Name,{BaseDN}

   PIV-I Card Authentication:

   For certificates with an Affiliated Organization:
   serialNumber=UUID, ou=Affiliated Organization Name,{Base DN}
   For certificates with no Affiliated Organization:
   serialNumber=UUID, ou=Unaffiliated, ou=Entity CA's Name,{Base DN}

3. Issuer CAs shall clearly indicate the organization administering the CMS in each PIV-I Content Signing Certificate.
4. Issuer CAs shall not include a Subscriber common name in a PIV-I Card Authentication subscriber Certificate.
5. Issuer CAs shall encode the UUID within the serialNumber attribute using the UUID string representation defined in Section 3 of RFC 4122.

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

3.1.2. Need for Names to be Meaningful

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

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

3.1.3. Anonymity or Pseudonymity of Subscribers

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

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

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

3.1.6. Recognition, Authentication, and Role of Trademarks

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

3.2. INITIAL IDENTITY VALIDATION

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

3.2.1. Method to Prove Possession of Private Key

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

3.2.2. Authentication of Organization Identity

Domain names included in a publicly trusted SSL Certificate must be verified in accordance with Section 3.2.2 of the Baseline Requirements.

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

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

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

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

3.2.3. Authentication of Individual Identity

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

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

Grid-only Certificates	Either the RA responsible for the grid community or a Trusted Agent must either review an identity document during a face-to-face meeting with the Applicant, or a Trusted Agent must attest that the Applicant is personally known to the Trusted Agent. If an identification document is used, the RA must retain sufficient information about the Applicant's identity in order to verify the Applicant at a later date.
Level 1 Client Certificates – Personal (email certificates)	Applicant's control over an email address (or any of the identity verification methods listed for a higher level client certificate).
Level 1 Client Certificates - Enterprise (email certificates)	Any one of the following: 1. In-person appearance before an RA or Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: - the ability to place or receive calls from a given number; or - the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: - the ability to obtain mail at the billing address used in the business relationship; or - verification of information established in previous transactions (e.g., previous order number); or - the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method required to verify identity for issuance of a Level 2, 3, or 4 Client Certificate
Level 2 Client Certificates	This level of assurance requires that the Issuer CA or RA verify the Applicant's identity using the possession of a reliable form of identification. Personal identifying information shall be compared with Applicant-provided information to confirm that the asserted name matches: (a) the name contained in the presented identification credential; (b) the individual's date of birth; and (c) a current address or personal telephone number sufficient to identify a unique individual. The Issuer CA or RA shall verify the Applicant's identity using one of the following four (4) methods: 1. In-person proofing before an RA or Trusted Agent (or entity certified by a State or National Government as authorized to confirm identities) with presentment of a valid current government-issued identity document that contains the Applicant's picture and either address of record or nationality (e.g. driver's license or Passport). Such authentication does not relieve the RA of its responsibility to

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

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

PIV-I Certificates	Issuer CAs shall only issue PIV-I Hardware Certificates to human subscribers. The RA or a Trusted Agent shall collect biometric data during the identity proofing and registration process that complies with [NIST SP 800-76] (see Appendix A): • An electronic facial image used for printing facial image on the card, as well as for performing visual authentication during card usage. The RA or Trusted Agent must collect a new facial image each time a card is issued; and • Two electronic fingerprints are stored on the card for automated authentication during card usage. The RA or Trusted Agent shall also require two identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document must be a valid, unexpired State or Federal Government-issued picture identification (ID). For all PIV-I Certificates, the use of an in-person antecedent is not applicable and the Applicant shall establish their identity no more than 30 days prior to initial certificate issuance.
EU Qualified Certificates	In-person verification of the Applicant's identity by appropriate means in accordance with national law. The entity performing the validation shall check the evidence of identity directly against a physical person or indirectly using means that provide equivalent assurance to physical presence.

* A Declaration of Identity consists of the following:

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

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

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

3.2.3.1. Authentication for Role-based Client Certificates

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

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

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

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

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

3.2.3.2. Authentication for Group Client Certificates

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

In addition, the Issuer CA or the RA shall:

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

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

3.2.3.3. Authentication of Devices with Human Sponsors

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

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

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

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

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

3.2.4. Non-verified Subscriber Information

Issuer CAs are not required to confirm that the common name in a Level 1 - Personal Client Certificate is the legal name of the Subscriber. Any other non-verified information included in a Certificate shall be designated as such in the Certificate. No unverified information shall be included in any Level 2, Level, 3, Level 4, PIV-I, Object Signing, EV, Federated Device, or EU Qualified Certificate.

3.2.5. Validation of Authority

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

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

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

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

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

Certificate	Routine Re-Key Authentication	Re-Verification Required
DV and OV SSL Certificates	Username and password	At least every 39 months
EV SSL Certificates	Username and password	According to the EV Guidelines
Subscriber Code Signing Certificates (Minimum Requirements and EV)	Username and password	At least every 39 months
Signing Authority EV Code Signing Certificates	Username and password	At least every 123 months
Timestamp EV Code Signing Certificates	Username and password	At least every 123 months
Object Signing Certificates	Username and password	At least every six years
Level 1 Client Certificates	Username and password	At least every nine years
Level 2 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Level 3 and 4 Client Certificates and PIV-I Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Federated Device and Federated Device-hardware	Current signature key or multi-factor authentication meeting NIST-800-63 Level 3	At least every nine years
IGTF Certificates	Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated Private Key	At least every 13 months. However, certificates associated with a Private Key restricted solely to a hardware token may be rekeyed or renewed for a period of up to 5 years
Authentication-Only Certificates	Username and password or with associated Private Key	None

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

3.3.2. Identification and Authentication for Re-key After Revocation

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

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

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

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

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

4.1.2. Enrollment Process and Responsibilities

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

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

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

4.2.2. Approval or Rejection of Certificate Applications

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

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

4.2.3. Time to Process Certificate Applications

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

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

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

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

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

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

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

4.4.2. Publication of the Certificate by the CA

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

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

No stipulation.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

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

4.5.2. Relying Party Public Key and Certificate Usage

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

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

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

An Issuer CA may renew a Certificate if:

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

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

4.6.2. Who May Request Renewal

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

4.6.3. Processing Certificate Renewal Requests

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

4.6.4. Notification of New Certificate Issuance to Subscriber

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

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6. Publication of the Renewal Certificate by the CA

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

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

No stipulation.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

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

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

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

4.7.2. Who May Request Certificate Rekey

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

4.7.3. Processing Certificate Rekey Requests

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

4.7.4. Notification of Certificate Rekey to Subscriber

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

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

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

4.7.6. Publication of the Rekeyed Certificate by the CA

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

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

No stipulation.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstance for Certificate Modification

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

4.8.2. Who May Request Certificate Modification

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

4.8.3. Processing Certificate Modification Requests

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

4.8.4. Notification of Certificate Modification to Subscriber

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

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

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

4.8.6. Publication of the Modified Certificate by the CA

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

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

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

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

1. The Subscriber requested revocation of its Certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised or misused;
4. The Subscriber or the cross-certified CA breached a material obligation under the CP, the CPS, or the relevant agreement;
5. Either the Subscriber's or the Issuer CA's obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The Applicant has lost its rights to a trademark or the domain name listed in the Certificate;

7. The Certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
8. The Issuer CA received a lawful and binding order from a government or regulatory body to revoke the Certificate;
9. The Issuer CA ceased operations and did not arrange for another certificate authority to provide revocation support for the Certificate;
10. The Issuer CA's right to manage Certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and to maintain the CRL/OCSP Repository);
11. Any information appearing in the Certificate was or became inaccurate or misleading;
12. The technical content or format of the Certificate presents an unacceptable security risk to application software vendors, Relying Parties, or others;
13. The Subscriber was added as a denied party or prohibited person to a blacklist, or is operating from a destination prohibited under U.S. law; or
14. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware or other harmful content, including any code that is downloaded onto a user's system without their consent.

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

If a Certificate expresses an organizational affiliation, the Issuer CA or the RA shall require the Affiliated Organization to inform it if the subscriber affiliation changes. If the Affiliated Organization no longer authorizes the affiliation of a Subscriber, then the Issuer CA shall revoke any Certificates issued to that Subscriber containing the organizational affiliation. If an Affiliated Organization terminates its relationship with the Issuer CA or RA such that it no longer provides affiliation information, the Issuer CA shall revoke all Certificates affiliated with that Affiliated Organization.

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

4.9.2. Who Can Request Revocation

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

4.9.3. Procedure for Revocation Request

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

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

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

4.9.4. Revocation Request Grace Period

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

4.9.5. Time within which CA Must Process the Revocation Request

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

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

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

4.9.6. Revocation Checking Requirement for Relying Parties

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

4.9.7. CRL Issuance Frequency

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

4.9.8. Maximum Latency for CRLs

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

4.9.9. On-line Revocation/Status Checking Availability

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

4.9.10. On-line Revocation Checking Requirements

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

4.9.11. Other Forms of Revocation Advertisements Available

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

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

4.9.12. Special Requirements Related to Key Compromise

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

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

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

4.10.2. Service Availability

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

4.10.3. Optional Features

No stipulation.

4.11. END OF SUBSCRIPTION

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

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices

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

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

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

An entity receiving Private Key escrow services shall:

1. Notify Subscribers that their Private Keys are escrowed,
2. Protect escrowed keys from unauthorized disclosure,
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys,
4. Release escrowed keys only for properly authenticated and authorized requests for recovery, and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

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

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

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

5.1.2. Physical Access

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

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

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

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

The Issuer CA shall make a person or group of persons explicitly responsible for making security checks. If a group of persons is responsible, the Issuer CA shall maintain a log that identifies who performed the security check. If the facility is not continuously attended, the last person to depart shall initial a sign-out sheet that indicates the date and time and asserts that all necessary physical protection mechanisms are in place and activated.

5.1.3. Power and Air Conditioning

The Issuer CA shall maintain a backup power supply and sufficient environmental controls to protect the CA systems and allow the CA to automatically finish pending operations and record the state of equipment before a lack of power or air conditioning causes a shutdown.

5.1.4. Water Exposures

The Issuer CA shall protect its CA equipment from water exposure.

5.1.5. Fire Prevention and Protection

The Issuer CA shall use facilities equipped with fire suppression mechanisms.

5.1.6. Media Storage

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

5.1.7. Waste Disposal

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

5.1.8. Off-site Backup

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

5.1.9. Certificate Status Hosting, CMS and External RA Systems

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

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

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

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

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

5.2.1.1. CA Administrators

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

5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel

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

5.2.1.3. System Administrator/ System Engineer (Operator)

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

5.2.1.4. Internal Auditor Role

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

5.2.2. Number of Persons Required per Task

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

5.2.3. Identification and Authentication for each Role

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

5.2.4. Roles Requiring Separation of Duties

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

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

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

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

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

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

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

5.3.2. Background Check Procedures

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

5.3.3. Training Requirements

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

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

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

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

5.3.4. Retraining Frequency and Requirements

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

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

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

5.3.7. Independent Contractor Requirements

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

5.3.8. Documentation Supplied to Personnel

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

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

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

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

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

Auditable Event
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs and OCSP entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
Installation of a Hardware Security Modules
Removal of HSMs
Destruction of HSMs
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
Backup of the internal CA database
Restoration from backup of the internal CA database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
Loading HSMs with Certificates
Shipment of HSMs
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA components
Access to a CA component
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions

Auditable Event
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CP or CPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

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

5.4.3. Retention Period for Audit Log

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

5.4.4. Protection of Audit Log

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

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

5.4.5. Audit Log Backup Procedures

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

5.4.6. Audit Collection System (internal vs. external)

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

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

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

5.5. RECORDS ARCHIVAL

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

5.5.1. Types of Records Archived

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

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

5.5.2. Retention Period for Archive

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

5.5.3. Protection of Archive

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

5.5.4. Archive Backup Procedures

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

5.5.5. Requirements for Time-stamping of Records

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

5.5.6. Archive Collection System (internal or external)

The Issuer CA shall collect archive information internally.

5.5.7. Procedures to Obtain and Verify Archive Information

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

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

5.6. KEY CHANGEOVER

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

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

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

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

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

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

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

5.7.3. Entity Private Key Compromise Procedures

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

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

5.7.4. Business Continuity Capabilities after a Disaster

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

5.8. CA OR RA TERMINATION

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

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

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

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

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

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

6.1.2. Private Key Delivery to Subscriber

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

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

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

6.1.3. Public Key Delivery to Certificate Issuer

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

6.1.4. CA Public Key Delivery to Relying Parties

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

DigiCert Certificates and all application software providers are permitted to redistribute any Root Certificate that is issued under this CP.

6.1.5. Key Sizes

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

The Issuer CA shall only issue end-entity Certificates that contain at least 2048-bit Public Keys for RSA, DSA, or Diffie-Hellman, or 224 bits for elliptic curve algorithms. The Issuer CA may require higher bit keys in its sole discretion. The Issuer CA shall only issue end-entity Certificates associated with PIV-I Cards that contain Public Keys and algorithms that conform to [NIST SP 800-78].

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

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

6.1.6. Public Key Parameters Generation and Quality Checking

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

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

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

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

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

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

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

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

PIV-I Content Signing certificates include an extended key usage of id-fpki-pivi-content-signing.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

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

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

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

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

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

6.2.1.1. Custodial Subscriber Key Stores

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

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

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

6.2.3. Private Key Escrow

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

6.2.4. Private Key Backup

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

The Issuer CA may provide backup services for Private Keys that are not required to be maintained in cryptographic hardware. Access to Private Key backups shall be secured in a manner that only the Subscriber can control the Private Key. The Issuer CA may not backup Level 4 subscriber private signature keys. The Issuer CA may not store backup keys in a plain text form outside of the cryptographic module. Storage that contains backup keys shall provide security controls that are consistent with the protection provided by the Subscriber's cryptographic module. The Issuer CA may require backup of PIV-I Content Signing private signature keys to facilitate disaster recovery, provided that all backup is performed under multi-person control.

6.2.5. Private Key Archival

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

6.2.6. Private Key Transfer into or from a Cryptographic Module

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

6.2.7. Private Key Storage on Cryptographic Module

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

6.2.8. Method of Activating Private Key

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

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

6.2.9. Method of Deactivating Private Key

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

6.2.10. Method of Destroying Private Key

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

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

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

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

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

Type	Private Key Use	Certificate Term
Root CA	20 years	25 years
Sub CA	12 years	15 years
FBCA-Cross-certified Sub CAs	6 years (period of key use for signing certificates)	10 years (key still signs CRLs, OCSP responses, and OCSP responder certificates)
IGTF Cross-certified Sub CA*	6 years	15 years
CRL and OCSP responder signing	3 years	31 days†
OV SSL	No stipulation	39 months
EV SSL	No stipulation	27 months
Code Signing Certificate issued to Subscriber under the Minimum Requirements for Code Signing Certificates or the EV Code Signing Guidelines	No stipulation	39 months
EV Code Signing Certificate issued to Signing Authority	No stipulation	123 months
Time Stamping Authority	15 months	135 months
Object Signing Certificate and Document Signing	No stipulation‡	123 months
FBCA and IGTF Client used for signatures (including EU Qualified Certificates)	36 months	36 months
FBCA and IGTF Client used for key management	36 months	36 months
Client for all other purposes (FBCA or IGTF compliant)	36 months	36 months
Client for all other purposes (non FBCA and	No stipulation	60 months

IGTF certs)		
PIV-I Content Signing[**]	36 months	9 years
PIV-I Cards	6 years	6 years
IGTF on hardware	60 months	13 months

[*] IGTF signing Certificates must have a lifetime that is at least twice the maximum lifetime of an end entity Certificate.

[†] OCSP responder and CRL signing Certificates associated with a PIV-I Certificate may only have a maximum certificate validity period of 31 days.

[‡] Code and content signers cross-certified with FBCA may use their Private Keys for three years; the lifetime of the associated Public Keys shall not exceed eight years.

[**] Subscriber Public Keys in Certificates that assert the PIV-I Content Signing OID in the extended key usage extension have a maximum usage period of nine years. The Private Keys corresponding to the Public Keys in these Certificates have a maximum usage period of three years. Expiration of PIV-I Content Signing Certificate shall be later than the expiration of the PIV-I Hardware and PIV-I Card Authentication Certificates.

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

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

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

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

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

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

6.4.2. Activation Data Protection

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

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

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

6.4.3. Other Aspects of Activation Data

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

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

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

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

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

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

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

A CMS must have the following computer security functions:

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

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

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

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

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

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

6.6.2. Security Management Controls

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

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

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

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

6.8. TIME-STAMPING

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

6.9. PIV-I CARDS

The following requirements apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards must use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and uses the PIV application identifier (AID).
2. The Issuer CA shall ensure that all PIV-I Cards conform to [NIST SP 800-731].
3. The Issuer CA shall only issue the mandatory X.509 Certificate for Authentication under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. The Issuer CA shall only issue PIV-I Certificates that conform to the PIV-I Profile.
5. The Issuer CA shall include an asymmetric X.509 Certificate for Card Authentication in each PIV-I card that:
    a. conforms to PIV-I Profile,
    b. conforms to [NIST SP 800-73], and
    c. is issued under the PIV-I Card Authentication policy.
6. The CMS shall include an electronic representation (as specified in SP 800-73 and SP 800-76) of the cardholder's facial image in each PIV-I card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. The CMS shall make its PIV-I Cards visually distinct from a Federal PIV Card to prevent creation of a fraudulent Federal PIV Card. At a minimum, the CMS shall not allow images or logos on a PIV-I Card to be placed within Zone 11, *Agency Seal*, as defined by [FIPS 201].
9. The CMS shall require the following items on the front of a card:

a. Cardholder facial image,
b. Cardholder full name,
c. Organizational Affiliation, if exists; otherwise the issuer of the card, and
d. Card expiration date.

10. The Issuer CA shall issue PIV-I cards with an expiration date that is six years or less.
11. All PIV-I Cards must not expire later than the PIV-I Content Signing Certificate on the card.
12. The Issuer CA shall include a policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID in the digital signature Certificate used to sign objects on the PIV-I Card. The PIV-I Content Signing Certificate must conform to the PIV-I Profile.
13. The Issuer CA and its RAs shall manage the PIV-I Content Signing Certificate and corresponding Private Key within a trusted Card Management System as defined herein.
14. At issuance, the RA shall activate and release the PIV-I Card to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.
15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys shall be set to be specific to each PIV-I Card. That is, each PIV-I Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78].

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

Issuer CAs shall issue X.509 version 3 Certificates.

7.1.2. Certificate Extensions

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

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

7.1.3. Algorithm Object Identifiers

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

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

ecdsa-with-SH256	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2 (3) 2 }
ecdsa-with-SHA384	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 3 }
ecdsa-with-SHA512	{ iso(1) member-body(2) us(840) ansi-X9-62 (10045) signatures(4) ecdsa-with-SHA2(3) 4 }

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

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

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

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

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

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

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

7.1.4. Name Forms

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

7.1.5. Name Constraints

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

7.1.6. Certificate Policy Object Identifier

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

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

Issuer CAs may include brief statements in the Policy Qualifier field of the Certificate Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

7.2.1. Version number(s)

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

7.2.2. CRL and CRL Entry Extensions

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

7.3. OCSP PROFILE

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

7.3.1. Version Number(s)

Issuer CAs shall support version 1 OCSP requests and responses.

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The policies in this CP are designed to meet or exceed the requirements of generally accepted and developing industry standards, including the EV Guidelines and the WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188"). For Issuer CAs chained to the FBCA, the auditor letter of compliance shall meet FPKIPA Audit Requirements. All Issuer CAs shall ensure that audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

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

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

The Issuer CA shall use an auditor that meets the following qualifications:

1. *Qualifications and experience*: Auditing must be the auditor's primary business function. The individual or at least one member of the audit group must be qualified as a Certified Information Systems Auditor (CISA), an AICPA Certified Information Technology

Professional (CPA.CITP), a Certified Internal Auditor (CIA), or have another recognized information security auditing credential.

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

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

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

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The Issuer CA shall utilize independent auditors that do not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against the Issuer CA.

8.4. TOPICS COVERED BY ASSESSMENT

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

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

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

8.7. SELF-AUDITS

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

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

Issuer CAs may charge fees for certificate issuance and renewal.

9.1.2. Certificate Access Fees

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

9.1.3. Revocation or Status Information Access Fees

No stipulation.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

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

9.2.2. Other Assets

No stipulation.

9.2.3. Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

Issuer CAs shall specify what constitutes confidential information in its CPS.

9.3.2. Information Not Within the Scope of Confidential Information

Issuer CAs may treat any information not listed as confidential in the CPS as public information.

9.3.3. Responsibility to Protect Confidential Information

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

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

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

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

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

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

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

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

9.4.7. Other Information Disclosure Circumstances
No stipulation.

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

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties
Issuer CAs must represent to DigiCert, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP, their CPS, and all applicable laws and regulations. For PIV-I, the Issuer CA shall maintain an agreement with Affiliated Organizations that includes obligations related to authorizing affiliation with Subscribers of PIV-I Certificates.

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

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

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information and communication to the Issuer CA and RA,
3. Confirm the accuracy of Certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify the Issuer CA if there is any actual or suspected misuse or compromise of the Private Key associated with the Public Key included in the Certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,
5. Use the Certificate only for authorized and legal purposes, consistent with the relevant CPS and Subscriber Agreement, including only installing SSL Certificates on servers accessible at

the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and

6. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

9.6.4. Relying Party Representations and Warranties

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

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

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

9.8. LIMITATIONS OF LIABILITY

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

9.9. INDEMNITIES

9.9.1. Indemnification by an Issuer CA

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

9.9.2. Indemnification by Subscribers

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

9.9.3. Indemnification by Relying Parties

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

9.10. TERM AND TERMINATION

9.10.1. Term

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

9.10.2. Termination

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

9.10.3. Effect of Termination and Survival

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

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

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

9.12.2. Notification Mechanism and Period

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

9.12.3. Circumstances under which OID Must Be Changed

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

9.13. DISPUTE RESOLUTION PROVISIONS

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

9.14. GOVERNING LAW

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

9.15. COMPLIANCE WITH APPLICABLE LAW

This CP is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, each Issuer CA shall meet the requirements of European data protection laws and shall establish and maintain appropriate technical and organization measures against unauthorized or unlawful processing of personal data and against the loss, damage, or destruction of personal data.

9.16. MISCELLANEOUS PROVISIONS

9.16.1. Entire Agreement

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

9.16.2. Assignment

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

9.16.3. Severability

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

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

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

9.16.5. Force Majeure

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

9.17. OTHER PROVISIONS

No stipulation.

DigiCert

Certification Practices Statement

DigiCert, Inc.
Version 4.11
February 23, 2017

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

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the DigiCert, Inc. ("DigiCert") Certification Practices Statement (CPS) that outlines the principles and practices related to DigiCert's certification and time-stamping services. This CPS applies to all entities participating in or using DigiCert's certificate and time-stamping services, excluding participants in DigiCert's Private PKI services, which are not cross-certified or publicly trusted. This CPS only addresses the actions of DigiCert and not those of third parties operating with cross certificates issued by DigiCert. Specific requirements regarding those Certificates are set forth in the individual agreements with the appropriate DigiCert customer or in that third party's own CPS.

This CPS describes the practices used to comply with the current versions of the following policies, guidelines, and requirements:

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

If any inconsistency exists between this CPS and the normative provisions of the foregoing policies, guidelines, and requirements ("Applicable Requirements"), then the Applicable Requirements take precedence over this CPS. Time-stamping services are provided according to IETF RFC 3161 and other technical standards.

This CPS is only one of several documents that control DigiCert's certification services. Other important documents include both private and public documents, such as the CP, DigiCert's agreements with its customers, Relying Party agreements, and DigiCert's privacy policy. DigiCert may provide additional certificate policies or certification practice statements. These supplemental policies and statements are available to applicable users or relying parties.

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 and time-stamping services within the DigiCert PKI. To preserve the outline specified by RFC 3647, section headings that do not apply are accompanied with the statement "Not applicable" or "No stipulation."

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certification Practices Statement and was first approved for publication on 9 August 2010 by the DigiCert Policy Authority (DCPA). The following revisions have been made to the original document:

Date	Changes	Version
23-February-2017	Updated address, made revisions related to the Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, and made other changes to update the CPS.	4.11
9-September-2016	Updated to: include Cybertrust CAs acquired from Verizon,	4.10

Date	Changes	Version
	clarify identity verification process, update document in accordance with FBCA CP v. 2.29 and sec. 9.6.3 of Baseline Requirements.	
1-June-2015	Updated CPS to conform to practices for backup, archival, CA key generation, and certificate acceptance.	4.09
1-April-2015	Minor changes made to update with CA/Browser Forum guidelines and for consistency with DigiCert CP v. 4.08	4.08
7-October-2014	Updated for consistency with DigiCert CP v. 4.07	4.07
14-May-2014	Updated practices to comply with new policy requirements and changes to the DirectTrust CP, Baseline Requirements, EV Guidelines, and EV Code Signing Guidelines.	4.06
2-May-2013	Updated mailing address. Also updated practices to comply with new policy requirements, the DirectTrust CP, changes to the Adobe program, and CAB Forum guidelines.	4.05
10-May-2012	Updated to include practices set forth in the Baseline Requirements, the current Mozilla CA Policy, EV Code Signing, the IGTF, and other policy bodies.	4.04
3-May-2011	IGTF Certificates added and minor updates made to several 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
9-August-2010	This version 4.0 replaces the DigiCert Certificate Policy and Certification Practices Statement, Version 3.08, dated May 29, 2009, and the DigiCert Certification Practice Statement for Extended Validation Certificates, Version 1.0.4, May 29, 2009.	4.0

The OID for DigiCert is joint-iso-ccitt (2) country (16) USA (840) US-company (1) DigiCert (114412). The OID-arc for this version 4 of the CPS is 2.16.840.1.114412.0.2.4. Subsequent revisions to this CPS might have new OID assignments. DigiCert issues Certificates and time-stamp tokens containing the following OIDs / OID arcs:

Digitally Signed Object	Object Identifier (OID)
Domain Vetted SSL Certificates and per the Baseline Requirements	2.16.840.1.114412.1.2 and/or 2.23.140.1.2.1 (CAB Forum Baseline Reqs.)
Organization Vetted SSL Certificates and per the Baseline Requirements	2.16.840.1.114412.1.1 and/or 2.23.140.1.2.2 (CAB Forum Baseline Reqs.)
Individual Vetted SSL Certificates per the Baseline Requirements	2.16.840.1.114412.1.1 and/or 2.23.140.1.2.3 (CAB Forum Baseline Reqs.)
Hotspot 2.0 OSU Server Certificates	2.16.840.1.114412.1.5
Federated Device Certificate	2.16.840.1.114412.1.11
Federated Device Hardware Certificate	2.16.840.1.114412.1.12
Issuer CA (where allowed by policy)	2.5.29.32.0 (anyPolicy)
Extended Validation SSL Certificates	2.16.840.1.114412.2 and/or 2.23.140.1.1(CAB Forum EV Guidelines)
Extended Validation SSL Certificates (issued under the Cybertrust Global Root)	1.3.6.1.4.1.6334.1.100.1 (originally registered by beTRUSTed)
Object Signing Certificates	2.16.840.1.114412.3
Code Signing Certificates	2.16.840.1.114412.3.1

Minimum Requirements for Code Signing	2.16.840.1.114412.3.1.1 and/or 2.23.140.1.4.1
Extended Validation Code Signing	2.16.840.1.114412.3.2
Windows Kernel Driver Signing	2.16.840.1.114412.3.11
Adobe Signing Certificate	2.16.840.1.114412.3.21
Client Certificate OID Arc	2.16.840.1.114412.4
Level 1 Certificates - Personal	2.16.840.1.114412.4.1.1
Level 1 Certificates - Enterprise	2.16.840.1.114412.4.1.2
Level 2 Certificates	2.16.840.1.114412.4.2
Level 3 Certificates - US	2.16.840.1.114412.4.3.1
Level 3 Certificates - CBP	2.16.840.1.114412.4.3.2
Level 4 Certificates - US	2.16.840.1.114412.4.4.1
Level 4 Certificates - CBP	2.16.840.1.114412.4.4.2
PIV-I OID Arc	2.16.840.1.114412.4.5
PIV-I Hardware - keys require activation by the PIV-I Cardholder (PIV Auth, Dig Sig and Key Management)	2.16.840.1.114412.4.5.1
PIV-I Card Authentication - keys do not require PIV-I Cardholder activation	2.16.840.1.114412.4.5.2
PIV-I Content Signing – use by PIV-I-compliant CMS	2.16.840.1.114412.4.5.3
Grid Certificate OID Arcs	2.16.840.1.114412.4.31 or 2.16.840.1.114412.31 (Grid-only arc)
IGTF Classic X.509 Authorities with secured infrastructure	2.16.840.1.114412.4.31.1 (Client w/ Public), 2.16.840.1.114412.31.4.1.1 (Client Grid Only), and/or 1.2.840.113612.5.2.2.1.x (IGTF)
IGTF Member Integrated X.509 Credential Services with Secured Infrastructure Certificates	2.16.840.1.114412.4.31.5 and/or 1.2.840.113612.5.2.2.5.x (IGTF)
IGTF Grid Host - Public Trust	2.16.840.1.114412.1.31.1
IGTF Grid-Only Host Certificate	2.16.840.1.114412.31.1.1.1, 1.2.840.113612.5.2.2.1.x (IGTF), and/or 1.2.840.113612.5.2.2.5.x (IGTF)
Authentication-Only Certificates	2.16.840.1.114412.6
Trusted Time-stamping	2.16.840.1.114412.7.1
Legacy arc	2.16.840.1.114412.81
Test arc	2.16.840.1.114412.99
EU OIDs	
EU Qualified Certificates ETSI TS 101 456	0.4.0.1456.1.2
EU QC on Secure Signature Creation Device ETSI TS 101 456	0.4.0.1456.1.1
ETSI TS 101 862 - Qualified Certificate Statements	0.4.0.1862.1.x
EU Qualified Time-stamping ETSI TS 102 023	0.4.0.2023.1.x

All OIDs mentioned above belong to their respective owners. The specific OIDs used when objects are signed pursuant to this CPS are indicated in the object's respective Certificate Policies extension. For instance, when DigiCert issues a Certificate containing one of the above-specified policy identifiers for "Baseline Requirements," "Minimum Requirements," or "Extended Validation," it asserts that the Certificate was issued and is managed in accordance with those applicable requirements. Commercial

Best Practices ("CBP") differs from "US" in that there are no trusted role citizenship requirements for an Issuer CA issuing under a CBP policy, whereas policies designated "US" must follow the citizenship practices set forth in Section 5.3.1.

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

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

DigiCert operates certification authorities (CAs) that issue digital certificates. As the operator of several CAs, DigiCert performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital Certificate, and maintaining, issuing, and publishing CRLs and OCSP responses. General information about DigiCert's products and services are available at www.digicert.com.

DigiCert owns and operates the GTE Cybertrust Global Root, the Baltimore Cybertrust Root, the Cybertrust Global Root CA, and the Verizon Global Root CA. In limited circumstances, these root CAs are used to issue cross Certificates to external third parties operating their own PKI. An "external subordinate CA" is an unaffiliated third party that is issued a subordinate CA Certificate by DigiCert where the Private Key associated with that CA Certificate is not maintained under the physical control of DigiCert. In accordance with requirements of the U.S. Federal PKI Policy Authority (FPKIPA), DigiCert notifies the FPKIPA prior to issuing a CA Certificate chaining to the Federal Bridge CA to an external subordinate CA. All external subordinate CAs are prohibited, either technically or contractually, from issuing Certificates to domain names or IP addresses that a Subscriber does not legitimately own or control (i.e. issuance for purposes of "traffic management" is prohibited), and external subordinate CAs are required to implement procedures that are at least as restrictive as those found herein.

DigiCert is also a time stamping authority (TSA) and provides proof-of-existence for data at an instant in time as described herein.

1.3.2. Registration Authorities and Other Delegated Third Parties

DigiCert may delegate the performance of certain functions to third party Registration Authorities (RA). The specific role of an RA or Delegated Third Party varies greatly between entities, ranging from simple translation services to actual assistance in gathering and verifying Applicant information. Some RAs operate identity management systems (IdMs) and may manage the certificate lifecycle for end-users. For IGTF Certificates, designated RAs are responsible for vetting the identity of each certificate applicant. DigiCert contractually obligates each Delegated Third Party to abide by the policies and industry standards that are applicable to that Delegated Third Party's delegated responsibilities.
RA personnel involved in the issuance of publicly-trusted SSL Certificates must undergo the skills and training required under Section 5.3.

1.3.3. Subscribers

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

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a Certificate and/or digital signature issued by DigiCert. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a Certificate. The location of the CRL distribution point is detailed within the Certificate.

1.3.5. Other Participants

Other participants include Accreditation Authorities (such as Policy Management Authorities, Federation Operators, Application Software Vendors, and applicable Community-of-Interest sponsors); Bridge CAs and CAs cross-certified with DigiCert's CAs that serve as trust anchors in other PKI communities; Card Management Systems and integrators (CMSs) that ensure proper operation and provisioning of PIV-I cards; and Time Source Entities, Time Stamp Token Requesters, and Time Stamp Verifiers involved in trusted time stamping. Accreditation Authorities are granted an unlimited right to re-distribute DigiCert's root Certificates and related information in connection with the accreditation.

When issuing PIV-I cards, DigiCert uses a Card Management Systems (CMS) that meets the requirements herein responsible for managing smart card token content. DigiCert does not issue Certificates to a CMS that include a PIV-I Hardware or PIV-I Card Authentication policy OID.

DigiCert has cross-certified with the Federal Bridge Certification Authority (FBCA). DigiCert also issues cross-Certificates to other third-party CAs.

1.4. CERTIFICATE USAGE

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

1.4.1. Appropriate Certificate Uses

Certificates issued pursuant to this CPS may be used for all legal authentication, encryption, access control, and digital signature purposes, as designated by the key usage and extended key usage fields found within the Certificate. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CPS.

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

Certificate	Appropriate Use
DV SSL Certificates	Used to secure online communication where the risks and consequences of data compromise are low, including non-monetary transactions or transactions with little risk of fraud or malicious access.
OV SSL Certificates	Used to secure online communication where the risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
EV SSL Certificates	Used to secure online communication where risks and consequences of data compromise are high, including transactions having high monetary value, risk of fraud, or where involving access to private information where the likelihood of malicious access is high.
Hotspot 2.0 OSU Server Certificates	Used to authenticate OSU Servers pursuant to the Wi-Fi Alliance's Hotspot 2.0 specification.
Federated Device Certificates	Similar to SSL Certificates above but for use as necessary in connection with cross-certified PKIs
Code Signing Certificates,	Establishes the identity of the Subscriber named in the Certificate and

including EV Code Signing	that the signed code has not been modified since signing.
Rudimentary Level 1 Client Certificates - Personal	Provides the lowest degree of assurance concerning identity of the individual and is generally used only to provide data integrity to the information being signed. These Certificates should only be used where the risk of malicious activity is low and if an authenticated transaction is not required.
Level 1 Client Certificates - Enterprise	Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 2 Client Certificates (FBCA basic assurance certificates)	Issued to identity-vetted individuals. Certificates specify if the name is a pseudonym. Used in environments where there are risks and consequences of data compromise, but such risks are not of major significance. Users are assumed not likely to be malicious.
Level 3 Client Certificates (FBCA medium certificates)	Used in environments where risks and consequences of data compromise are moderate, including transactions having substantial monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is substantial.
Level 4 Client Certificates (FBCA medium hardware Certificates)	Used in environments where risks and consequences of data compromise are high, including transactions having high monetary value or risk of fraud or involving access to private information where the likelihood of malicious access is high.
Direct Certificates	Used to transfer health care information in accordance with the Direct Protocol adopted by the ONC. Direct Certificates are issued as Level 2 or Level 3 Certificates.
Authentication Only	Used where the identity of the certificate holder is irrelevant and where the risk of unauthorized access to a secure site is low.
IGTF and Grid-only Certificates	Support identity assertions and system authentication amongst participants in the International Grid Trust Federation. IGTF Certificates include those issued as publicly-trusted client Certificates and those issued under the Grid-only arc.
PIV-I Hardware PIV-I Card Authentication PIV-I Content Signing PIV-I Digital Signature PIV-I Key Management	This level is relevant to environments where risks and consequences of data compromise are moderate. This may include contactless smart card readers where use of an activation PIN is not practical. Personal Identity Verification – Interoperable (PIV-I) cards are intended to technically interoperate with Federal PIV Card readers and applications. The requirements associated with PIV-I Hardware and PIV-I Content Signing are identical to Level 4 Certificates except where specifically noted herein. PIV-I Content Signing policy is reserved for Certificates used by the Card Management System (CMS) to sign the PIV-I card security objects
Adobe Signing Certificates	Used to sign Adobe documents and show that the portion of the document signed by the author has not been modified since signing.
Time Stamp Token	Used to identify the existence of data at a set period of time.

1.4.2. Prohibited Certificate Uses

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

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

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

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

1.5.2. Contact Person

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

1.5.3. Person Determining CPS Suitability for the Policy

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

1.5.4. CPS Approval Procedures

The DCPA approves the CPS and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with the CP, by either updating the entire CPS or by publishing an addendum. The DCPA determines whether an amendment to this CPS is consistent with the CP, requires notice, or an OID change. *See also* Section 9.10 and Section 9.12 below.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

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

"Applicant" means an entity applying for a Certificate.

"Application Software Vendor" means a software developer whose software displays or uses DigiCert Certificates and distributes DigiCert's root Certificates.

"CAB Forum" is defined in section 1.1.

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

"Certificate Approver" is defined in the EV Guidelines.

"Certificate Requester" is defined in the EV Guidelines.

“Contract Signer” is defined in the EV Guidelines.

“Direct Address” means an email address conforming to the Applicability Statement for Secure Health Transport.

“Direct Address Certificate” means a Certificate containing an entire Direct Address.

“Direct Device Certificate” means a Certificate containing the FQDN or IP address of a host machine.

“Direct Organizational Certificate” means a Certificate containing only the domain name portion of a Direct Address.

“EV Guidelines” is defined in section 1.1.

“Key Pair” means a Private Key and associated Public Key.

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

“**PIV-I Profile**” means the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards, Ver. 1.1, Date: May 5 2015.

“Private Key” means the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

“Public Key” means the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

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

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

“Relying Party Agreement” means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using DigiCert’s Repository. The Relying Party Agreement is available for reference through a DigiCert online repository.

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

“Subscriber” means either the entity identified as the subject in the Certificate or the entity that is receiving DigiCert’s time-stamping services.

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

“WebTrust” means the current version of CPA Canada’s WebTrust Program for Certification Authorities.

“WebTrust EV Program” means the additional audit procedures specified for CAs that issue EV Certificates by CPA Canada to be used in conjunction with its WebTrust Program for Certification Authorities.

1.6.2. Acronyms

AATL	Adobe Approved Trust List
CA	Certificate Authority or Certification Authority
CAA	Certification Authority Authorization
CAB	”CA/Browser” as in “CAB Forum”
CMS	Card Management System
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
CT	Certificate Transparency
DBA	Doing Business As (also known as "Trading As")
DCPA	DigiCert Policy Authority
DV	Domain Validated
ETSI	European Telecommunications Standards Institute
EU	European Union
EV	Extended Validation
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HISP	Health Information Service Provider
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
ISSO	Information System Security Officer
IETF	Internet Engineering Task Force
IGTF	International Grid Trust Federation
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
IV	Individual Validated
MICS	Member-Integrated Credential Service (IGTF)
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Healthcare (U.S.)
OSU	Online Sign-Up (Wi-Fi Alliance Hotspot 2.0)
OV	Organization Validated
PIN	Personal Identification Number (e.g. a secret access code)
PIV-I	Personal Identity Verification-Interoperable
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
RFC	Request for Comments (at IETF.org)
SAN	Subject Alternative Name
SHA	Secure Hashing Algorithm
SSCD	Secure Signature Creation Device
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
TSA	Time Stamping Authority

TST	Time-Stamp Token
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

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

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

DirectTrust Community X.509 Certificate Policy, v.1.2.1

FBCA Supplementary Antecedent, In-Person Definition

Wi-Fi Alliance Hotspot 2.0 Release 2 Online Signup Certificate Policy Specification (Hotspot 2.0 CP)

X.509 Certificate Policy for the Federal Bridge Certification Authority, v. 2.28

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

DigiCert makes its root Certificates, revocation data for issued digital Certificates, CPs, CPSs, Relying Party Agreements, and standard Subscriber Agreements available in public repositories.

DigiCert's legal repository for most services is located at http://www.digicert.com/ssl-cps-repository.htm. DigiCert's publicly trusted root Certificates and its CRLs and OCSP responses are available through online resources 24 hours a day, 7 days a week with systems described in Section 5 to minimize downtime.

2.2. PUBLICATION OF CERTIFICATION INFORMATION

The DigiCert certificate services and the repository are accessible through several means of communication:

1. On the web: www.digicert.com (and via URIs included in the certificates themselves)
2. By email to admin@digicert.com
3. By mail addressed to: DigiCert, Inc., Suite 500, 2801 N. Thanksgiving Way, Lehi, Utah 84043
4. By telephone Tel: 1-801-877-2100
5. By fax: 1-801-705-0481

2.3. TIME OR FREQUENCY OF PUBLICATION

CA Certificates are published in a repository as soon as possible after issuance. CRLs for end-user Certificates are issued at least once per day. CRLs for CA Certificates are issued at least every 6 months (every 31 days for offline CAs chaining to the Federal Bridge CA), and also within 18 hours if a CA Certificate is revoked. Under special circumstances, DigiCert may publish new CRLs prior to the scheduled issuance of the next CRL. (See Section 4.9 for additional details.)

New or modified versions of the CP, this CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

Read-only access to the repository is unrestricted. Logical and physical controls prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a non-null subject Distinguished Name (DN) that complies with ITU X.500 standards except that DigiCert may issue a Level 1 Certificate with a null subject DN if it includes at least one alternative name form that is marked critical. When DNs are used, common names must respect namespace uniqueness requirements and must not be misleading. This does not preclude the use of pseudonymous Certificates, except where stated otherwise under Section 3.1.3.

DigiCert issues EV SSL/TLS Certificates to .onion domains in accordance with Appendix F of the EV Guidelines.

DigiCert issues OSU Server Certificates with subject alternative names that contain: (1) OSU Server FQDN(s) and (2) Friendly Name(s) that identify the wifi service provider, in accordance with section 3.4 of the Hotspot 2.0 CP.

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

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

For Certificates with an Affiliated Organization:

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

For Certificates with no Affiliated Organization:

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

Each PIV-I Content Signing certificate also clearly indicates the organization administering the CMS. PIV-I Card Authentication subscriber Certificate do not include a Subscriber common name.

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

For Certificates with an Affiliated Organization:

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

For Certificates with no Affiliated Organization:

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

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

The subject name in each EU Qualified Certificate complies with section 3.1.2 of RFC 3739

3.1.2. Need for Names to be Meaningful

DigiCert uses distinguished names that identify both the entity (i.e. person, organization, device, or object) that is the subject of the Certificate and the entity that is the issuer of the Certificate. DigiCert only allows directory information trees that accurately reflect organization structures.

3.1.3. Anonymity or Pseudonymity of Subscribers

Generally, DigiCert does not issue anonymous or pseudonymous Certificates; however, for IDNs, DigiCert may include the Punycode version of the IDN as a subject name. DigiCert may also issue other pseudonymous end-entity Certificates if they are not prohibited by policy and any applicable name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

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

3.1.5. Uniqueness of Names

The uniqueness of each subject name in a Certificate is enforced as follows:

SSL Server Certificates	Inclusion of the domain name in the Certificate. Domain name uniqueness is controlled by the Internet Corporation for Assigned Names and Numbers (ICANN).
Client Certificates	Requiring a unique email address or a unique organization name combined/associated with a unique serial integer.
IGTF and Grid-only Device Certificates	For device Certificates, an FQDN is included in the appropriate fields. For other Certificates, DigiCert may append a unique ID to a name listed in the Certificate.
Code Signing Certificates (including CDS Certificates)	Requiring a unique organization name and address or a unique organization name combined/associated with a unique serial integer.
Time Stamping	Requiring a unique hash and time or unique serial integer assigned to the time stamp

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers may not request Certificates with content that infringes on the intellectual property rights of another entity.

For OSU Server Certificates, DigiCert conducts a trademark search of logos and Friendly Names in relevant mark registration databases, such as the U.S. Patent and Trademark Office or WIPO, to confirm an applicant's right to use a particular trademark. Based on the results of such search(es), DigiCert issues an OSU Server Certificate with one or more logotype extensions containing the hash algorithm and hash value of logos associated with the service provider. If an applicant does not have a friendly name or logo available, DigiCert may include a logo and friendly name specified by the Wi-Fi Alliance.

Unless otherwise specifically stated in this CPS, DigiCert does not verify an Applicant's right to use a trademark and does not resolve trademark disputes. DigiCert may 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

DigiCert establishes that the Applicant holds or controls the Private Key corresponding to the Public Key by performing signature verification or decryption on data purported to have been digitally signed or encrypted with the Private Key by using the Public Key associated with the certificate request.

3.2.2. Authentication of Organization Identity

DV SSL Server Certificates	DigiCert validates the Applicant's right to use or control the domain names that will be listed in the Certificate using one or more of the following procedures: 1. Relying on publicly available records from the Domain Name Registrar, such as WHOIS or other DNS record information;

	2. Communicating with one of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed in the technical, registrant, or administrative contact field of the domain's Registrar record; 3. Requiring a practical demonstration of domain control (e.g., requiring the Applicant to make a specified change to a DNS zone file or a live page on the given domain); and/or 4. A domain authorization letter, provided the letter contains the signature of an authorized representative of the domain holder, a date that is on or after the certificate request, a list of the approved fully-qualified domain name(s), and a statement granting the Applicant the right to use the domain names in the Certificate. DigiCert also contacts the domain name holder using a reliable third-party data source to confirm the authenticity of the domain authorization letter; and/or 5. A similar procedure that offers an equivalent level of assurance in the Applicant's ownership, control, or right to use the Domain Name. DigiCert verifies an included country code using (a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address; (b) the ccTLD of the requested Domain Name; or (c) information provided by the Domain Name Registrar.
IV and OV SSL Server, OSU Server, Object Signing, and Device Certificates (excluding device Certificates issued under the Grid-only arc)	DigiCert validates the Applicant's right to use or control the Domain Name(s) that will be listed in the Certificate using the DV SSL Server Certificate validation procedures above. DigiCert also verifies the identity and address of the Applicant using: 1. a reliable third party/government databases or through communication with the entity or jurisdiction governing the organization's legal creation, existence, or recognition; 2. a site visit; 3. an attestation letter that is signed by an accountant, lawyer, government official, or other reliable third party; or 4. for address only, a utility bill, bank statement, credit card statement, tax document, or other reliable form of identification. DigiCert verifies any DBA included in a Certificate using a third party or government source, attestation letter, or reliable form of identification.
Device Certificates issued under the Grid-only arc	An RA or Trusted Agent validates the applicant's information in accordance with an RPS (or similar document) applicable to the community of interest.
EV SSL and EV Code Signing Certificates	Information concerning organization identity related to the issuance of EV Certificates is validated in accordance with the EV Guidelines.
Level 1 Client Certificates - Enterprise	DigiCert verifies organizational control over the email domain using authentication procedures similar to those used when establishing

	domain control before issuance of a DV or OV SSL Server Certificate.
Level 2, 3, and 4 Client Certificates	If the Certificate contains organization information, DigiCert obtains documentation from the organization sufficient to confirm that the individual has an affiliation with the organization named in the Certificate.
PIV-I	For certificate requests that assert an organizational affiliation between a human subscriber and an organization, DigiCert verifies the organization's identity and legal existence and the organization is required to enter into an agreement authorizing or recognizing that affiliation and requiring that the organization request revocation of the Certificate when that affiliation ends.

DigiCert maintains and utilizes a scoring system to flag certificate requests that potentially present a higher risk of fraud. Those certificate requests that are flagged "high risk" receive additional scrutiny or verification prior to issuance, which may include obtaining additional documentation from or additional communication with the Applicant.

Before issuing an SSL Certificate with a domain name that has not been previously verified as within the scope of an RA's or other Delegated Third Party's allowed domain names, DigiCert establishes that the RA or Delegated Third Party has the right to use the Domain Name by independently verifying the authorization with the domain owner, as described above, or by using other reliable means, such as performing a DNS lookup to determine whether there is a matching DNS record that points to the Delegated Third Party's IP address or domain namespace.

DigiCert verifies the organization name, address, legal existence, and authorization for CA Certificates that cross-certify with the FBCA.

3.2.3. Authentication of Individual Identity

If a Certificate will contain the identity of an individual, then DigiCert or an RA validates the identity of the individual using the following procedures:

Certificate	Validation
IV SSL Server Certificates and Object Signing Certificates (issued to an individual)	1. DigiCert or the RA obtains a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, driver's license, military ID, national ID, or equivalent document type). DigiCert or the RA inspects the copy for any indication of alteration or falsification. 2. DigiCert may additionally cross-check the Applicant's name and address for consistency with available third party data sources. 3. If further assurance is required, then the Applicant must provide an additional form of identification, such as recent utility bills, financial account statements, credit card, an additional ID credential, or equivalent document type. 4. DigiCert or the RA confirms that the Applicant is able to receive communication by telephone, postal mail/courier, or fax. If DigiCert cannot verify the Applicant's identity using the procedures described above, then the Applicant must submit a Declaration of Identity that is witnessed and signed by a

	Registration Authority, Trusted Agent, notary, lawyer, accountant, postal carrier, or any entity certified by a State or National Government as authorized to confirm identities.
Device Certificate Sponsors	See section 3.2.3.3
OSU Server Certificates	DigiCert verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
EV Certificates issued to a business entity	As specified in the EV Guidelines
Grid-only Certificates	Either the RA responsible for the grid community or a Trusted Agent obtains an identity document during a face-to-face meeting with the Applicant, or a Trusted Agent attests that the Applicant is personally known to the Trusted Agent. The RA must retain sufficient information about the applicant's identity to prove upon DigiCert's request that the applicant was properly identified.
Authentication-Only Certificates	The entity controlling the secure location must represent that the certificate holder is authorized to access the location.
Level 1 Client Certificates – Personal (email Certificates)	DigiCert or an RA verifies Applicant's control of the email address or website listed in the Certificate.
Level 1 Client Certificates - Enterprise	Any one of the following: 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent with presentment of an identity credential (e.g., driver's license or birth certificate). 2. Using procedures similar to those used when applying for consumer credit and authenticated through information in consumer credit databases or government records, such as: a. the ability to place or receive calls from a given number; or b. the ability to obtain mail sent to a known physical address. 3. Through information derived from an ongoing business relationship with the credential provider or a partner company (e.g., a financial institution, airline, employer, or retail company). Acceptable information includes: a. the ability to obtain mail at the billing address used in the business relationship; b. verification of information established in previous transactions (e.g., previous order number); or c. the ability to place calls from or receive phone calls at a phone number used in previous business transactions. 4. Any method used to verify the identity of an Applicant for a Level 2, 3, or 4 Client Certificate.
Level 2 Client Certificates and IGTF Classic/MICS Certificates	The CA or an RA confirms that the following are consistent with the application and sufficient to identify a unique individual: (a) the name on the government-issued photo-ID referenced below; (b) date of birth; and

	(c) current address or personal telephone number. 1. In-person appearance before a person performing identity proofing for a Registration Authority or a Trusted Agent (or entity certified by a state, federal, or national entity as authorized to confirm identities) with presentment of a reliable form of current government-issued photo ID. 2. The Applicant must possess a valid, current, government-issued, photo ID. The Registration Authority or Trusted Agent performing identity proofing must obtain and review, which may be through remote verification, the following information about the Applicant: (i) name, date of birth, and current address or telephone number; (ii) serial number assigned to the primary, government-issued photo ID; and (iii) one additional form of ID such as another government-issued ID, an employee or student ID card number, telephone number, a financial account number (e.g., checking account, savings account, loan or credit card), or a utility service account number (e.g., electricity, gas, or water) for an address matching the applicant's residence. Identity proofing through remote verification may rely on database record checks with an agent/institution or through credit bureaus or similar databases. DigiCert or an RA may confirm an address by issuing credentials in a manner that confirms the address of record or by verifying knowledge of recent account activity associated with the Applicant's address and may confirm a telephone number by sending a challenge-response SMS text message or by recording the applicant's voice during a communication after associating the telephone number with the applicant in records available to DigiCert or the RA. 3. Where DigiCert or an RA has a current and ongoing relationship with the Applicant, identity may be verified through the exchange of a previously exchanged shared secret (e.g., a PIN or password) that meets or exceeds NIST SP 800-63 Level 2 entropy requirements, provided that: (a) identity was originally established with the degree of rigor equivalent to that required in 1 or 2 above using a government-issued photo-ID, and (b) an ongoing relationship exists sufficient to ensure the Applicant's continued personal possession of the shared secret. 4. Any of the methods used to verify the identity of an applicant for a DigiCert Level 3 or 4 Client Certificate.
Level 3 Client Certificates	In-person proofing before an RA, Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. The information must be collected and stored in a secure manner. Required identification consists of one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card,

	tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The person performing identity proofing examines the credentials and determines whether they are authentic and unexpired and checks the provided information (name, date of birth, and current address) to ensure legitimacy. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. DigiCert or the RA reviews and keeps a record of the Declaration of Identity. DigiCert also employs the in-person antecedent process, defined in FBCA Supplementary Antecedent, In-Person Definition, to meet this in-person identity proofing requirement. Under this definition, historical in-person identity proofing is sufficient if (1) it meets the thoroughness and rigor of in-person proofing described above, (2) supporting ID proofing artifacts exist to substantiate the antecedent relationship, and (3) mechanisms are in place that bind the individual to the asserted identity. In one use case, the Applicant (e.g. an employee) has been identified previously by an employer using USCIS Form I-9 and is bound to the asserted identity remotely through the use of known attributes or shared secrets. In another use case, DigiCert uses a third party Identity Verification Provider that constructs a real-time, five-question process, based on multiple historic antecedent databases, and the applicant is given two minutes to answer at least four of the five questions correctly. See FBCA Supplementary Antecedent, In-Person Definition. The identity of the Applicant must be established no earlier than 30 days prior to initial certificate issuance.
Level 4 Client Certificates (Biometric ID Certificates)	In-person proofing before an RA, Trusted Agent, or an entity certified by a state, federal, or national entity that is authorized to confirm identities. A certified entity must forward the collected information directly to an RA in a secure manner. The Applicant must supply one unexpired Federal/National Government-issued Picture I.D. (e.g. a passport), a REAL ID, or two unexpired Non-Federal Government I.D.s, one of which must be a photo I.D.. Acceptable forms of government ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, military ID, or similar photo identification document. See e.g. USCIS Form I-9. The entity collecting the credentials must also obtain at least one form of biometric data (e.g. photograph or fingerprints) to ensure that the Applicant cannot repudiate the application. The person performing identity verification for DigiCert or the RA examines the credentials for authenticity and validity. The Applicant signs a Declaration of Identity, defined below, to which the person performing identity proofing attests. DigiCert or the RA reviews and keeps a record of the Declaration of Identity. Use of an in-person antecedent is not allowed. The identity of the Applicant must be established by in-person proofing no earlier than 30 days prior to initial certificate issuance. Level 4 Client Certificates

	are issued in a manner that confirms the Applicant's address.
PIV-I Certificates	PIV-I Hardware Certificates are only issued to human subscribers. The following biometric data is collected by DigiCert, an RA, or a Trusted Agent during the identity proofing and registration process: 1. An electronic facial image used for printing facial image on the card and for visual authentication during card usage. A new facial image is collected each time a card is issued; and 2. Two electronic fingerprints are stored on the card for automated authentication during card usage. The Subscriber must also present two identity source documents in original form that come from the list of acceptable documents included in Form I-9. At least one document must be a valid, unexpired State or Federal Government-issued picture identification (ID). For PIV-I, the use of an in-person antecedent is not applicable. Identity is established no more than 30 days prior to initial certificate issuance.
EU Qualified Certificates	Using identity and attribute validation procedures in accordance with national law. Evidence of identity is checked directly against a physical person or indirectly using means which provides equivalent assurance to physical presence.

A Declaration of Identity consists of:

1. the identity of the person performing the verification;
2. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law, the signature on the declaration may be either a handwritten or digital signature using a Certificate that is of equal or higher level of assurance as the credential being issued;
3. unique identifying number(s) from the Applicant's identification document(s), or a facsimile of the ID(s);
4. the date of the verification; and
5. a declaration of identity by the Applicant that is signed (in handwriting or using a digital signature that is of equivalent or higher assurance than the credential being issued) in the presence of the person performing the verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

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

For in-person identity proofing at Levels 3 and 4 and for PIV-I, DigiCert may rely on an entity certified by a state, federal, or national entity as authorized to confirm identities may perform the authentication on behalf of the RA. The certified entity should forward the information collected from the applicant directly to the RA in a secure manner.

3.2.3.1. Authentication for Role-based Client Certificates

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

DigiCert verifies the identity of the individual requesting a role-based Certificate (the sponsor) in accordance with Section 3.2.3 before issuing a role-based Certificate. The sponsor must hold a DigiCert-issued client individual Certificate at the same or higher assurance level as the role-based Certificate. If the Certificate is a pseudonymous Certificate cross-certified with the FBCA that identifies subjects by their organizational roles, then DigiCert or an RA validates that the individual either holds that role or has the authority to sign on behalf of the role.

Regarding the issuance of role-based Certificates, this CPS requires compliance with all provisions of DigiCert's CP regarding key generation, private key protection, and Subscriber obligations.

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

3.2.3.2. Authentication for Group Client Certificates

DigiCert issues group Certificates (a Certificate that corresponds to a Private Key that is shared by multiple Subscribers) if several entities are acting in one capacity and if non-repudiation is not required. Direct Address Certificates and Direct Organizational Certificates are used as group Certificates consistent with applicable requirements of the Direct Program. DigiCert or the RA records the information identified in Section 3.2.3 for a sponsor before issuing a group Certificate. The sponsor must be at least an Information Systems Security Officer (ISSO) or of the equivalent rank or greater within the organization.

The sponsor is responsible for ensuring control of the Private Key. The sponsor must maintain and continuously update a list of Subscribers with access to the Private Key and account for the time period during which each Subscriber had control of the key. Group Certificates may list the identity of an individual in the subjectName DN provided that the subjectName DN field also includes a text string, such as "Direct Group Cert," so that the Certificate specifies the subject is a group and not a single individual. Client Certificates issued in this way to an organization are always considered group client Certificates.

3.2.3.3. Authentication of Devices with Human Sponsors

DigiCert issues Level 1, 2, 3 or 4 Client and Federated Device Certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device has a human sponsor who provides:

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

If the Certificate's sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive Certificates. Each sponsor is required to provide proof that the device is still under the sponsor's control or responsibility on request. 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.

3.2.4. Non-verified Subscriber Information

The common name of a Level 1 - Personal Client Certificates is not verified as the legal name of the Subscriber. DV SSL Server Certificates do not include a verified organizational identity. Any other non-verified information included in a Certificate is designated as such in the Certificate. Unverified information is never included in a Level 2, Level, 3, Level 4, PIV-I, Object Signing, EV SSL, Federated Device, or EU Qualified Certificate.

3.2.5. Validation of Authority

The authorization of a certificate request is verified as follows:

Certificate	Verification
DV SSL Server Certificate	The request is verified with an authorized contact listed with the Domain Name Registrar, through a person with control over the domain, or through an out-of-band confirmation with the applicant. A person with control over the domain name is considered to have authority to request DV SSL Certificates, including any individual with access to one more of the following email addresses: webmaster@domain.com, administrator@domain.com, admin@domain.com, hostmaster@domain, postmaster@domain, or any address listed as a contact field of the domain's Domain Name Registrar record.
OV SSL Server and Federated Device Certificates	The request is verified using a Reliable Method of Communication, in accordance with the Baseline Requirements.
OSU Server Certificates	DigiCert verifies that the requester is a duly authorized representative of the organization as an employee, partner, member, agent, etc., and is authorized to act on behalf of the organization.
EV Certificates	The request is verified in accordance with the EV Guidelines.
Object Signing Certificates and Adobe Signing Certificates	If the Certificate 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 (email Certificates)	The request is verified through the email address listed in the Certificate.
Level 1 Client Certificates – Enterprise (email Certificates)	The request is verified with a person who has technical or administrative control over the domain and the email address to be listed in the Certificate.
Client Certificates Levels 2, 3 and 4 and PIV-I Certificates	The organization named in the Certificate confirms to DigiCert or an RA that the individual is authorized to obtain the Certificate. The organization is required to request revocation of the Certificate when that affiliation ends.
Direct Address and Direct Organization Certificates	The entity named in the Certificate authorizes a HISP to order the Certificate and use the related Private Key on the entity's behalf. The HISP ISSO is responsible for tracking access to and ensuring proper use of the Private Key.
IGTF Certificates	An authorized individual approves the certificate request. For device Certificates, the RA retains contact information for each device's registered owner. The device owner is required to notify the RA and request revocation if the device sponsor is no longer authorized to use the device or the FQDN in the Certificate.
EU Qualified Certificates	DigiCert verifies that the individual is associated with the organization listed in the Certificate (if any) and that the organization consented to the issuance of the Certificate.

An organization may limit who is authorized to request Certificates by sending a request to DigiCert. A request to limit authorized individuals is not effective until approved by DigiCert. DigiCert will respond to an organization's verified request for DigiCert's list of its authorized requesters.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request re-key of a Certificate prior to a Certificate's expiration. After receiving a request for re-key, DigiCert creates a new Certificate with the same certificate contents except for a new Public Key and, optionally, an extended validity period. If the Certificate has an extended validity period, DigiCert may perform some revalidation of the Applicant but may also rely on information previously provided or obtained.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
DV and OV SSL Server and Device Certificates	Username and password	At least every 39 months
EV SSL Certificates	Username and password	According to the EV Guidelines
Subscriber Code Signing Certificates (Minimum Requirements and EV)	Username and password	At least every 39 months
Signing Authority EV Code Signing Certificates	Username and password	At least every 123 months
Timestamp EV Code Signing Certificates	Username and password	At least every 123 months
Object Signing Certificates (including Adobe Signing Certificates)	Username and password	At least every six years
Level 1 Client Certificates	Username and password	At least every nine years
Level 2 Client Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Level 3 and 4 Client Certificates and PIV-I Certificates	Current signature key or multi-factor authentication meeting NIST SP 800-63 Level 3	At least every nine years
Federated Device and Federated Device-hardware	Current signature key or multi-factor authentication meeting NIST-800-63 Level 3	At least every nine years
IGTF Certificates	Username and password, RA attestation after comparison of identity documents, re-authenticate through an approved IdM, or through associated Private Key	At least every 13 months. However, Certificates associated with a Private Key restricted solely to a hardware token may be rekeyed or renewed for a period of up to 5 years
Authentication-Only Certificates	Username and password or with associated Private Key	None

DigiCert does not re-key a Certificate without additional authentication if doing so would allow the Subscriber to use the Certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

If a Certificate was revoked for any reason other than a renewal, update, or modification action, then the Subscriber must undergo the initial registration process prior to rekeying the Certificate.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

DigiCert or an RA authenticates all revocation requests. DigiCert may authenticate revocation requests by referencing the Certificate's Public Key, regardless of whether the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

Either the Applicant or an individual authorized to request Certificates on behalf of the Applicant may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DigiCert.

EV Certificate requests must be submitted by an authorized Certificate Requester and approved by a Certificate Approver. The certificate request must be accompanied by a signed (in writing or electronically) Subscriber Agreement from a Contract Signer.

DigiCert does not issue Certificates to entities on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

4.1.2. Enrollment Process and Responsibilities

In no particular order, the enrollment process includes:

1. Submitting a certificate application,
2. Generating a Key Pair,
3. Delivering the Public Key of the Key Pair to DigiCert,
4. Agreeing to the applicable Subscriber Agreement, and
5. Paying any applicable fees.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After receiving a certificate application, DigiCert or an RA verifies the application information and other information in accordance with Section 3.2. During the initial validation process, DigiCert checks the DNS for the existence of a CAA record. If a CAA record exists that does not list DigiCert as an authorized CA, DigiCert verifies that the applicant has authorized issuance, despite the CAA record. If an RA assists in the verification, the RA must create and maintain records sufficient to establish that it has performed its required verification tasks and communicate the completion of such performance to DigiCert. After verification is complete, DigiCert evaluates the corpus of information and decides whether or not to issue the Certificate. As part of this evaluation, DigiCert checks the Certificate against an internal database of previously revoked Certificates and rejected certificate requests to identify suspicious certificate requests. If some or all of the documentation used to support an application is in a language other than English, a DigiCert employee, RA, or agent skilled in the language performs the final cross-correlation and due diligence.

DigiCert considers a source's availability, purpose, and reputation when determining whether a third party source is reasonably reliable. DigiCert does not consider a database, source, or form of identification reasonably reliable if DigiCert or the RA is the sole source of the information.

4.2.2. Approval or Rejection of Certificate Applications

DigiCert rejects any certificate application that DigiCert or an RA cannot verify. DigiCert may also reject a certificate application if DigiCert believes that issuing the Certificate could damage or diminish DigiCert's reputation or business.

Except for Enterprise EV Certificates, EV Certificate issuance approval requires two separate DigiCert validation specialists. The second validation specialist cannot be the same individual who collected the documentation and originally approved the EV Certificate. The second validation specialist reviews the collected information and documents any discrepancies or details that require further explanation. The second validation specialist may require additional explanations and documents prior to authorizing the

Certificate's issuance. Enterprise RAs may perform the final cross-correlation and due diligence described herein using a single person representing the Enterprise RA. If satisfactory explanations and/or additional documents are not received within a reasonable time, DigiCert will reject the EV Certificate request and notify the Applicant accordingly.

If the certificate application is not rejected and is successfully validated in accordance with this CPS, DigiCert will approve the certificate application and issue the Certificate. DigiCert is not liable for any rejected Certificate and is not obligated to disclose the reasons for a rejection. Rejected Applicants may re-apply. Subscribers are required to check the Certificate's contents for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

Under normal circumstances, DigiCert verifies an Applicant's information and issues a digital Certificate within a reasonable time frame. Issuance time frames are greatly dependent on when the Applicant provides the details and documentation necessary to complete validation. For non-EV SSL Certificates, DigiCert will usually complete the validation process and issue or reject a certificate application within two working days after receiving all of the necessary details and documentation from the Applicant, although events outside of the control of DigiCert can delay the issuance process.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

DigiCert confirms the source of a certificate request before issuance. DigiCert does not issue end entity Certificates directly from its root Certificates. DigiCert logs its EV Certificates in two or more Certificate Transparency databases. See RFC 6962. Databases and CA processes occurring during certificate issuance are protected from unauthorized modification. After issuance is complete, the Certificate is stored in a database and sent to the Subscriber.

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

DigiCert may deliver Certificates in any secure manner within a reasonable time after issuance. Generally, DigiCert delivers Certificates via email to the email address designated by the Subscriber during the application process.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Subscribers are solely responsible for installing the issued Certificate on the Subscriber's computer or hardware security module. Certificates are considered accepted 30 days after the Certificate's issuance, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.4.2. Publication of the Certificate by the CA

DigiCert publishes all CA Certificates in its repository. DigiCert publishes end-entity Certificates by delivering them to the Subscriber.

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

RAs may receive notification of a Certificate's issuance if the RA was involved in the issuance process.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Subscribers are contractually obligated to protect their Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

4.5.2. Relying Party Public Key and Certificate Usage

Relying Parties may only use software that is compliant with X.509, IETF RFCs, and other applicable standards. DigiCert does not warrant that any third party software will support or enforce the controls and requirements found herein.

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. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate. Any warranties provided by DigiCert are only valid if a Relying Party's reliance was reasonable and if the Relying Party adhered to the Relying Party Agreement set forth in the DigiCert repository.

A Relying Party should rely on a digital signature or SSL/TLS handshake only if:

1. the digital signature or SSL/TLS session was created during the operational period of a valid Certificate and can be verified by referencing a valid Certificate,
2. the Certificate is not revoked and the Relying Party checked the revocation status of the Certificate prior to the Certificate's use by referring to the relevant CRLs or OCSP responses, and
3. the Certificate is being used for its intended purpose and in accordance with this CPS.

Before relying on a time-stamp token, a Relying Party must:

1. verify that the time-stamp token has been correctly signed and that the Private Key used to sign the time-stamp token has not been compromised prior to the time of the verification,
2. take into account any limitations on the usage of the time-stamp token indicated by the time-stamp policy, and
3. take into account any other precautions prescribed in this CPS or elsewhere.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

DigiCert may renew a Certificate if:

1. the associated Public Key has not reached the end of its validity period,
2. the Subscriber and attributes are consistent, and
3. the associated Private Key remains uncompromised.

DigiCert may also renew a Certificate if a CA Certificate is re-keyed or as otherwise necessary to provide services to a customer. DigiCert may notify Subscribers prior to a Certificate's expiration date. Certificate renewal requires payment of additional fees.

4.6.2. Who May Request Renewal

Only the certificate subject or an authorized representative of the certificate subject may request renewal of the Subscriber's Certificates. For Certificates cross-certified with the FBCA, renewal requests are only accepted from certificate subjects, PKI sponsors, or RAs. DigiCert may renew a Certificate without a corresponding request if the signing Certificate is re-keyed.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are generally the same as those used during the Certificate's original issuance. DigiCert may elect to reuse previously verified information in its sole discretion but will refresh any information that is older than the periods specified in Section 3.3.1. DigiCert may refuse to renew a Certificate if it cannot verify any rechecked information. If an individual is renewing a client Certificate and the relevant information has not changed, then DigiCert does not require any additional identity vetting. Some device platforms, e.g. Apache, allow renewed use of the Private Key. If the Private Key and domain information have not changed, the Subscriber may renew the SSL Certificate using a previously issued Certificate or provided CSR.

4.6.4. Notification of New Certificate Issuance to Subscriber

DigiCert may deliver the Certificate in any secure fashion, typically by email or by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the Certificate.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed Certificates are considered accepted 30 days after the Certificate's renewal, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.6.6. Publication of the Renewal Certificate by the CA

DigiCert publishes a renewed Certificate by delivering it to the Subscriber. All renewed CA Certificates are published in DigiCert's repository.

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

RAs may receive notification of a Certificate's renewal if the RA was involved in the issuance process.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a Certificate consists of creating a new Certificate with a new Public Key and serial number while keeping the subject information the same. The new Certificate may have a different validity date, key identifiers, CRL and OCSP distribution points, and signing key. After re-keying a Certificate, a PIV-I Certificate, or a federated device Certificate, DigiCert may revoke the old Certificate but may not further re-key, renew, or modify the previous Certificate. Subscribers requesting re-key should identify and authenticate themselves as permitted by section 3.3.1.

4.7.2. Who May Request Certificate Rekey

DigiCert will only accept re-key requests from the subject of the Certificate or the PKI sponsor. DigiCert may initiate a certificate re-key at the request of the certificate subject or in DigiCert's own discretion.

4.7.3. Processing Certificate Rekey Requests

DigiCert will only accept re-key requests from the subject of the Certificate or the PKI sponsor. If the Private Key and any identity and domain information in a Certificate have not changed, then DigiCert can issue a replacement Certificate using a previously issued Certificate or previously provided CSR. DigiCert re-uses existing verification information unless re-verification and authentication is required under section 3.3.1 or if DigiCert believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

DigiCert notifies the Subscriber within a reasonable time after the Certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued Certificates are considered accepted 30 days after the Certificate is rekeyed, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.7.6. Publication of the Issued Certificate by the CA

DigiCert publishes rekeyed Certificates by delivering them to Subscribers.

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

RAs may receive notification of a Certificate's rekey if the RA was involved in the issuance process.

4.8. CERTIFICATE MODIFICATION

4.8.1. Circumstances for Certificate Modification

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

4.8.2. Who May Request Certificate Modification

DigiCert modifies Certificates at the request of certain certificate subjects or in its own discretion. DigiCert does not make certificate modification services available to all Subscribers.

4.8.3. Processing Certificate Modification Requests

After receiving a request for modification, DigiCert verifies any information that will change in the modified Certificate. DigiCert will only issue the modified Certificate after completing the verification process on all modified information. DigiCert will not issue a modified Certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.4. Notification of Certificate Modification to Subscriber

DigiCert notifies the Subscriber within a reasonable time after the Certificate issues.

4.8.5. Conduct Constituting Acceptance of a Modified Certificate

Modified Certificates are considered accepted 30 days after the Certificate is modified, or earlier upon use of the Certificate when evidence exists that the Subscriber used the Certificate.

4.8.6. Publication of the Modified Certificate by the CA

DigiCert publishes modified Certificates by delivering them to Subscribers.

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

RAs may receive notification of a Certificate's modification if the RA was involved in the issuance process.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, DigiCert verifies the identity and authority of the entity requesting revocation. DigiCert may revoke any Certificate in its sole discretion, including if DigiCert believes that:

1. The Subscriber requested revocation of its Certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the Certificate or the Private Key used to sign the Certificate was compromised or misused;
4. The Subscriber breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement;
5. Either the Subscriber's or DigiCert's obligations under the CP or CPS are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised;
6. The Subscriber, sponsor, or other entity that was issued the Certificate has lost its rights to a name, trademark, device, IP address, domain name, or other attribute that was associated with the Certificate;
7. A wildcard Certificate was used to authenticate a fraudulently misleading subordinate domain name;
8. The Certificate was not issued in accordance with the CP, CPS, or applicable industry standards;

9. DigiCert received a lawful and binding order from a government or regulatory body to revoke the Certificate;
10. DigiCert ceased operations and did not arrange for another certificate authority to provide revocation support for the Certificates;
11. DigiCert's right to manage Certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
12. Any information appearing in the Certificate was or became inaccurate or misleading;
13. The technical content or format of the Certificate presents an unacceptable risk to application software vendors, Relying Parties, or others;
14. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;
15. For Adobe Signing Certificates, Adobe has requested revocation; or
16. For code-signing Certificates, the Certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

DigiCert always revokes a Certificate if the binding between the subject and the subject's Public Key in the certificate is no longer valid or if an associated Private Key is compromised.

DigiCert will revoke a cross-Certificate if the cross-certified entity (including DigiCert) no longer meets the stipulations of the corresponding policies, as indicated by policy OIDs listed in the policy mapping extension of the cross-Certificate.

4.9.2. Who Can Request Revocation

Any appropriately authorized party, such as a recognized representative of a subscriber or cross-signed partner, may request revocation of a Certificate. DigiCert may revoke a Certificate without receiving a request and without reason. Third parties may request certificate revocation for problems related to fraud, misuse, or compromise. Certificate revocation requests must identify the entity requesting revocation and specify the reason for revocation.

4.9.3. Procedure for Revocation Request

DigiCert processes a revocation request as follows:

1. DigiCert logs the identity of entity making the request or problem report and the reason for requesting revocation. DigiCert may also include its own reasons for revocation in the log.
2. DigiCert may request confirmation of the revocation from a known administrator, where applicable, via out-of-band communication (e.g., telephone, fax, etc.).
3. If the request is authenticated as originating from the Subscriber, DigiCert revokes the Certificate.
4. For requests from third parties, DigiCert personnel begin investigating the request within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
    a. the nature of the alleged problem,
    b. the number of reports received about a particular Certificate or website,
    c. the identity of the complainants (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
    d. relevant legislation.
5. If DigiCert determines that revocation is appropriate, DigiCert personnel revoke the Certificate and update the CRL.

DigiCert maintains a continuous 24/7 ability to internally respond to any high priority revocation requests. If appropriate, DigiCert forwards complaints to law enforcement.

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

4.9.4. Revocation Request Grace Period

Subscribers are required to request revocation within one day after detecting the loss or compromise of the Private Key. DigiCert may grant and extend revocation grace periods on a case-by-case basis. DigiCert reports the suspected compromise of its CA Private Key and requests revocation to both the policy authority and operating authority of the superior issuing CA within one hour of discovery.

4.9.5. Time within which CA Must Process the Revocation Request

DigiCert will revoke a CA Certificate within one hour after receiving clear instructions from the DCPA. Other Certificates are revoked as quickly as practical after validating the revocation request, generally within the following time frames:

1. Certificate revocation requests for publicly-trusted Certificates are processed within 18 hours after their receipt,
2. Revocation requests received two or more hours before CRL issuance are processed before the next CRL is published, and
3. Revocation requests received within two hours of CRL issuance are processed before the following CRL is published.

4.9.6. Revocation Checking Requirement for Relying Parties

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

4.9.7. CRL Issuance Frequency

DigiCert uses its offline root CAs to publish CRLs for its intermediate CAs at least every 6 months. For an offline CA that has been cross-signed by the Federal Bridge CA and only issues CA Certificates, certificate-status-checking certificates, or internal administrative Certificates, DigiCert issues a CRL at least every 31 days. All other CRLs are published at least every 24 hours. If a Certificate is revoked for reason of key compromise, an interim CRL is published as soon as feasible, but no later than 18 hours after receipt of the notice of key compromise.

4.9.8. Maximum Latency for CRLs

CRLs for Certificates issued to end entity subscribers are posted automatically to the online repository within a commercially reasonable time after generation, usually within minutes of generation. Irregular, interim, or emergency CRLs and all CRLs for CAs chaining to the Federal Bridge are posted within four hours after generation. Regularly scheduled CRLs are posted prior to the nextUpdate field in the previously issued CRL of the same scope.

4.9.9. On-line Revocation/Status Checking Availability

DigiCert makes certificate status information available via OCSP for SSL and PIV-I Certificates. OCSP may not be available for other kinds of Certificates. Where OCSP support is required by the applicable CP, OCSP responses are provided within a commercially reasonable time and no later than six seconds after the request is received, subject to transmission latencies over the Internet.

4.9.10. On-line Revocation Checking Requirements

A relying party must confirm the validity of a Certificate in accordance with section 4.9.6 prior to relying on the Certificate.

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. If a Certificate is revoked because of compromise, DigiCert will issue a new CRL within 18 hours after receiving notice of the compromise.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked Certificate remains on the CRL until one additional CRL is published after the end of the Certificate's validity period, except for revoked EV Code Signing Certificates, which remain on the CRL for at least 365 days following the Certificate's validity period. OCSP information for subscriber Certificates is updated at least every four days. OCSP information for subordinate CA Certificates is updated at least every 12 months and within 24 hours after revoking the Certificate.

4.10.2. Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3. Optional Features

OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION

A Subscriber's subscription service ends if its Certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

4.12.1. Key Escrow and Recovery Policy Practices

DigiCert never escrows CA Private Keys.

DigiCert may escrow Subscriber key management keys to provide key recovery services. DigiCert encrypts and protects escrowed Private Keys using the same or a higher level of security as used to generate and deliver the Private Key. For Certificates cross-certified with the FBCA, third parties are not permitted to hold the Subscriber signature keys in trust.

DigiCert allows Subscribers and other authorized entities to recover escrowed (decryption) Private Keys. DigiCert uses multi-person controls during key recovery to prevent unauthorized access to a Subscriber's escrowed Private Keys. DigiCert accepts key recovery requests:

1. From the Subscriber or Subscriber's organization, if the Subscriber has lost or damaged the private-key token;
2. From the Subscriber's organization, if the Subscriber is not available or is no longer part of the organization that contracted with DigiCert for Private Key escrow;

3. From an authorized investigator or auditor, if the Private Key is part of a required investigation or audit;
4. From a requester authorized by a competent legal authority to access the communication that is encrypted using the key;
5. From a requester authorized by law or governmental regulation; or
6. From an entity contracting with DigiCert for escrow of the Private Key when key recovery is mission critical or mission essential.

Entities using DigiCert's key escrow services are required to:

1. Notify Subscribers that their Private Keys are escrowed;
2. Protect escrowed keys from unauthorized disclosure;
3. Protect any authentication mechanisms that could be used to recover escrowed Private Keys;
4. Release an escrowed key only after making or receiving (as applicable) a properly authorized request for recovery; and
5. Comply with any legal obligations to disclose or keep confidential escrowed keys, escrowed key-related information, or the facts concerning any key recovery request or process.

4.12.2. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

DigiCert performs its CA and TSA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make DigiCert's CA and TSA operations inaccessible to non-trusted personnel. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to DigiCert's operations.

5.1.2. Physical Access

DigiCert protects its equipment (including certificate status servers and CMS equipment containing PIV-I Content Signing keys) from unauthorized access and implements physical controls to reduce the risk of equipment tampering. The secure parts of DigiCert CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals.

Access to secure areas of the buildings requires the use of an "access" or "pass" card. The buildings are equipped with motion detecting sensors, and the exterior and internal passageways of the buildings are under constant video surveillance. DigiCert securely stores all removable media and paper containing sensitive plain-text information related to its CA operations in secure containers in accordance with its Data Classification Policy.

5.1.2.1. Data Center

The data centers where DigiCert's CA and TSA systems operate have security personnel on duty full time (24 hours per day, 365 days per year). Access to the data centers housing the CA and TSA platforms requires two-factor authentication—the individual must have an authorized access card and pass biometric access control authenticators. These biometric authentication access systems log each use of the access card. DigiCert deactivates and securely stores its CA equipment when not in use. Activation data must either be memorized or recorded and stored in a manner commensurate with the security afforded the cryptographic module. Activation data is never stored with the cryptographic module or removable hardware associated with equipment used to administer DigiCert's Private Keys. Cryptographic hardware includes a mechanism to lock the hardware after a certain number of failed login attempts.

The DigiCert data centers are continuously attended. However, if DigiCert ever becomes aware that a data center is to be left unattended or has been left unattended for an extended period of time, DigiCert personnel will perform a security check of the data center to verify that:

1. DigiCert's equipment is in a state appropriate to the current mode of operation,
2. Any security containers are properly secured,
3. Physical security systems (e.g., door locks) are functioning properly, and
4. The area is secured against unauthorized access.

DigiCert's administrators are responsible for making these checks and must sign off that all necessary physical protection mechanisms are in place and activated. The identity of the individual making the check is logged.

5.1.2.2. Support and Vetting Room

Controlled access and keyed-lock doors secure the support and vetting rooms where DigiCert personnel perform identity vetting and other RA functions. Access card use is logged by the building security system. The room is equipped with motion-activated video surveillance cameras.

5.1.3. Power and Air Conditioning

Data centers have primary and secondary power supplies that ensure continuous and uninterrupted access to electric power. Uninterrupted power supplies (UPS) and diesel generators provide redundant backup power. DigiCert monitors capacity demands and makes projections about future capacity requirements to ensure that adequate processing power and storage are available.

DigiCert's data center facilities use multiple load-balanced HVAC systems for heating, cooling, and air ventilation through perforated-tile raised flooring to prevent overheating and to maintain a suitable humidity level for sensitive computer systems.

5.1.4. Water Exposures

The cabinets housing DigiCert's CA and TSA systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

5.1.5. Fire Prevention and Protection

The data centers are equipped with fire suppression mechanisms.

5.1.6. Media Storage

DigiCert protects its media from accidental damage and unauthorized physical access. Backup files are created on a daily basis. DigiCert's backup files are maintained at locations separate from DigiCert's primary data operations facility.

5.1.7. Waste Disposal

All unnecessary copies of printed sensitive information are shredded on-site before disposal. All electronic media are zeroized (all data is overwritten with binary zeros so as to prevent the recovery of the data) using programs meeting U.S. Department of Defense requirements.

5.1.8. Off-site Backup

DigiCert maintains at least one full backup and makes regular backup copies of any information necessary to recover from a system failure. Backup copies of CA Private Keys and activation data are stored for disaster recovery purposes off-site in safe deposit boxes located inside federally insured financial institutions and are accessible only by trusted personnel.

5.1.9. Certificate Status Hosting, CMS and External RA Systems

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

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Personnel acting in trusted roles include CA, TSA, and RA system administration personnel, and personnel involved with identity vetting and the issuance and revocation of Certificates. The functions and duties performed by persons in trusted roles are distributed so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI or TSA operations. All personnel in trusted roles must be free from conflicts of interest that might prejudice the impartiality of the DigiCert PKI's operations. Trusted roles are appointed by senior management. A list of personnel appointed to trusted roles is maintained and reviewed annually.

Persons acting in trusted roles are only allowed to access a CMS after they are authenticated using a method commensurate with issuance and control of PIV-I Hardware.

5.2.1.1. CA Administrators

The CA Administrator installs and configures the CA software, including key generation, key backup, and key management. The CA Administrator performs and securely stores regular system backups of the CA system. Administrators do not issue Certificates to Subscribers.

5.2.1.2. Registration Officers – CMS, RA, Validation and Vetting Personnel

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

5.2.1.3. System Administrators/ System Engineers (Operator)

The System Administrator / System Engineer installs and configures system hardware, including servers, routers, firewalls, and network configurations. The System Administrator / System Engineer also keeps CA, CMS and RA systems updated with software patches and other maintenance needed for system stability and recoverability.

5.2.1.4. Internal Auditors

Internal Auditors are responsible for reviewing, maintaining, and archiving audit logs and performing or overseeing internal compliance audits to determine if DigiCert, an Issuer CA, or RA is operating in accordance with this CPS or an RA's Registration Practices Statement.

5.2.2. Number of Persons Required per Task

DigiCert requires that at least two people acting in a trusted role (one the CA Administrator and the other not an Internal Auditor) take action requiring a trusted role, such as activating DigiCert's Private Keys, generating a CA Key Pair, or backing up a DigiCert Private Key. The Internal Auditor may serve to fulfill the requirement of multiparty control for physical access to the CA system but not logical access.

No single individual has the capability to issue a PIV-I credential.

5.2.3. Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA, TSA, and RA systems before they are allowed access to systems necessary to perform their trusted roles.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. Those performing authorization functions such as the verification of information in certificate applications and approvals of certificate applications and revocation requests,
2. Those performing backups, recording, and record keeping functions;
3. Those performing audit, review, oversight, or reconciliation functions; and

4. Those performing duties related to CA/TSA key management or CA/TSA administration.

To accomplish this separation of duties, DigiCert specifically designates individuals to the trusted roles defined in Section 5.2.1 above. DigiCert appoints individuals to only one of the Registration Officer, Administrator, Operator, or Internal Auditor roles. Individuals designated as Registration Officer or Administrator may perform Operator duties, but an Internal Auditor may not assume any other role. DigiCert's systems identify and authenticate individuals acting in trusted roles, restrict an individual from assuming multiple roles, and prevent any individual from having more than one identity.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

The DCPA is responsible and accountable for DigiCert's PKI operations and ensures compliance with this CPS and the CP. DigiCert's personnel and management practices provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. All trusted roles for CAs issuing Federated Device Certificates, Client Certificates at Levels 3-US and 4-US (which are intended for interoperability through the Federal Bridge CA at id-fpki-certpcy-mediumAssurance and id-fpki-certpcy-mediumHardware), and PIV-I Certificates are held by citizens of the United States. An individual performing a trusted role for an RA may be a citizen of the country where the RA is located. There is no citizenship requirement for personnel performing trusted roles associated with the issuance of other kinds of Certificates.

Management and operational support personnel involved in time-stamp operations possess experience with information security and risk assessment and knowledge of time-stamping technology, digital signature technology, mechanisms for calibration of time stamping clocks with UTC, and security procedures. The DCPA ensures that all individuals assigned to trusted roles have the experience, qualifications, and trustworthiness required to perform their duties under this CPS.

5.3.2. Background Check Procedures

DigiCert verifies the identity of each employee appointed to a trusted role and performs a background check prior to allowing such person to act in a trusted role. DigiCert requires each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee verifies the individual's identity using government-issued photo identification (e.g., passports and/or driver's licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual's identity is being verified). Background checks include employment history, education, character references, social security number, previous residences, driving records and criminal background. Checks of previous residences are over the past three years. All other checks are for the previous five years. The highest education degree obtained is verified regardless of the date awarded. Based upon the information obtained during the background check, the human resources department makes an adjudication decision, with the assistance of legal counsel when necessary, as to whether the individual is suitable for the position to which they will be assigned. Background checks are refreshed and re-adjudication occurs at least every ten years.

5.3.3. Training Requirements

DigiCert provides skills training to all employees involved in DigiCert's PKI and TSA operations. The training relates to the person's job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by DigiCert,
3. authentication and verification policies and procedures,
4. DigiCert security principles and mechanisms,
5. disaster recovery and business continuity procedures,
6. common threats to the validation process, including phishing and other social engineering tactics, and
7. applicable industry and government guidelines.

Training is provided via a mentoring process involving senior members of the team to which the employee belongs.

DigiCert maintains records of who received training and what level of training was completed. Registration Officers must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges. All Registration Officers are required to pass an internal examination on the EV Guidelines and the Baseline Requirements prior to validating and approving the issuance of Certificates. Where competence is demonstrated in lieu of training, DigiCert maintains supporting documentation.

5.3.4. Retraining Frequency and Requirements

Employees must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. DigiCert makes all employees acting in trusted roles aware of any changes to DigiCert's operations. If DigiCert's operations change, DigiCert will provide documented training, in accordance with an executed training plan, to all employees acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

DigiCert employees and agents failing to comply with this CPS, whether through negligence or malicious intent, are subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by management for unauthorized or inappropriate actions, the person will be immediately removed from the trusted role pending management review. After management has reviewed and discussed the incident with the employee involved, management may reassign that employee to a non-trusted role or dismiss the individual from employment as appropriate.

5.3.7. Independent Contractor Requirements

Independent contractors who are assigned to perform trusted roles are subject to the duties and requirements specified for such roles in this Section 5.3 and are subject to sanctions stated above in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties, including a copy of the CP, this CPS, EV Guidelines, and other technical and operational documentation needed to maintain the integrity of DigiCert's CA operations. Personnel are also given access to information on internal systems and security documentation, identity vetting policies and procedures, discipline-specific books, treatises and periodicals, and other information.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

DigiCert's systems require identification and authentication at system logon with a unique user name and password. Important system actions are logged to establish the accountability of the operators who initiate such actions.

DigiCert enables all essential event auditing capabilities of its CA and TSA applications in order to record the events listed below. If DigiCert's applications cannot automatically record an event, DigiCert implements manual procedures to satisfy the requirements. For each event, DigiCert records the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. DigiCert records the precise time of any significant TSA events. All event records are available to auditors as proof of DigiCert's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by the system
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
KEY GENERATION
Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)
PRIVATE KEY LOAD AND STORAGE
The loading of Component Private Keys
All access to certificate subject Private Keys retained within the CA for key recovery purposes
TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE
SECRET KEY STORAGE
The manual entry of secret keys used for authentication
PRIVATE AND SECRET KEY EXPORT
The export of private and secret keys (keys used for a single session or message are excluded)
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Certificate issuance
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL AND REJECTION
CA CONFIGURATION
Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
REVOCATION PROFILE MANAGEMENT
All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT
All changes to the certificate revocation list profile
Generation of CRLs and OCSP entries
TIME STAMPING
Clock synchronization
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System, PKI Application, or Hardware Security Module

Auditable Event
Removal or Destruction of HSMs
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set or modify passwords
Backup or restoration of the internal CA database
File manipulation (e.g., creation, renaming, moving)
Posting of any material to a repository
Access to the internal CA database
All certificate compromise notification requests
Loading HSMs with Certificates
Shipment of HSMs
Zeroizing HSMs
Re-key of the Component
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Personnel access to secure area housing CA or TSA component
Access to a CA or TSA component
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of a CPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

At least once every two months, a DigiCert administrator reviews the logs generated by DigiCert's systems, makes system and file integrity checks, and conducts a vulnerability assessment. The administrator may perform the checks using automated tools. During these checks, the administrator (1) checks whether anyone has tampered with the log, (2) scans for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepares a written summary of the review. Any anomalies or irregularities found in the logs are investigated. The summaries include recommendations to DigiCert's operations management committee and are made available to DigiCert's auditors upon request. DigiCert documents any actions taken as a result of a review.

5.4.3. Retention Period for Audit Log

DigiCert retains audit logs on-site until after they are reviewed. The individuals who remove audit logs from DigiCert's CA systems are different than the individuals who control DigiCert's signature keys.

5.4.4. Protection of Audit Log

CA audit log information is retained on equipment until after it is copied by a system administrator. DigiCert's CA and TSA systems are configured to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period and are retained securely on-site until transferred to a backup site. DigiCert's off-site storage location is a safe and secure location that is separate from the location where the data was generated.

DigiCert makes time-stamping records available when required to prove in a legal proceeding that DigiCert's time-stamping services are operating correctly. Audit logs are made available to auditors upon request.

5.4.5. Audit Log Backup Procedures

DigiCert makes regular backup copies of audit logs and audit log summaries and sends a copy of the audit log off-site on a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes begin on system startup and end 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, DigiCert's Administrators and the DCPA shall be notified and the DCPA will consider suspending the CA's or RA's operations until the problem is remedied.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

DigiCert performs annual 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. DigiCert also routinely assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that DigiCert has in place to control such risks. DigiCert's Internal Auditors review the security audit data checks for continuity. DigiCert's audit log monitoring tools 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

DigiCert complies with all record retention policies that apply by law. DigiCert includes sufficient detail in all archived records to show that a Certificate or time-stamp token was issued in accordance with this CPS.

5.5.1. Types of Records Archived

DigiCert retains the following information in its archives (as such information pertains to DigiCert's CA / TSA operations):

1. Accreditations of DigiCert,
2. CP and CPS versions,
3. Contractual obligations and other agreements concerning the operation of the CA / TSA,
4. System and equipment configurations, modifications, and updates,
5. Rejection or acceptance of a certificate request,
6. Certificate issuance, rekey, renewal, and revocation requests,
7. Sufficient identity authentication data to satisfy the identification requirements of Section 3.2, including information about telephone calls made for verification purposes,
8. Any documentation related to the receipt or acceptance of a Certificate or token,
9. Subscriber Agreements,
10. Issued Certificates,
11. A record of certificate re-keys,
12. CRLs for CAs cross-certified with the Federal Bridge CA,
13. Data or applications necessary to verify an archive's contents,

14. Compliance auditor reports,
15. Changes to DigiCert's audit parameters,
16. Any attempt to delete or modify audit logs,
17. Key generation, destruction, storage, backup, and recovery,
18. Access to Private Keys for key recovery purposes,
19. Changes to trusted Public Keys,
20. Export of Private Keys,
21. Approval or rejection of a revocation request,
22. Appointment of an individual to a trusted role,
23. Destruction of a cryptographic module,
24. Certificate compromise notifications,
25. Remedial action taken as a result of violations of physical security, and
26. Violations of the CP or CPS.

5.5.2. Retention Period for Archive

DigiCert retains archived data associated with Level 3 or Level 4, federated device, and PIV-I Certificates for at least 10.5 years. DigiCert, or the RA supporting issuance, archives data for other certificate types for at least 7.5 years.

5.5.3. Protection of Archive

Archive records are stored at a secure off-site location and are maintained in a manner that prevents unauthorized modification, substitution, or destruction. Archives are not released except as allowed by the DCPA or as required by law. DigiCert maintains any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If DigiCert needs to transfer any media to a different archive site or equipment, DigiCert will maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives will occur in a secure manner.

5.5.4. Archive Backup Procedures

On at least an annual basis, DigiCert creates an archive disk of the data listed in section 5.5.1 by grouping the data types together by source into separate, compressed archive files. Each archive file is hashed to produce checksums that are stored separately for integrity verification at a later date. DigiCert stores the archive disk in a secure off-site location for the duration of the set retention period. RAs create and store archived records in accordance with the applicable documentation retention policy.

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 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 compressed archive file with the file checksum originally stored for that file, 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

Key changeover procedures enable the smooth transition from expiring CA Certificates to new CA Certificates. Towards the end of a CA Private Key's lifetime, DigiCert ceases using the expiring CA Private Key to sign Certificates and uses the old Private Key only to sign CRLs and OCSP responder Certificates. A new CA signing Key Pair is commissioned and all subsequently issued Certificates and CRLs are signed with the new private signing key. Both the old and the new Key Pairs may be concurrently active. This key changeover process helps minimize any adverse effects from CA certificate expiration. The corresponding new CA Public Key Certificate is provided to subscribers and relying parties through the delivery methods detailed in Section 6.1.4. Where DigiCert has cross-certified another CA that is in the process of a key rollover, DigiCert obtains a new CA Public Key (PKCS#10) or new CA Certificate from the other CA and distributes a new CA cross Certificate following the procedures described above.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

DigiCert maintains incident response procedures to guide personnel in response to security incidents, natural disasters, and similar events that may give rise to system compromise. DigiCert reviews, tests, and updates its incident response plans and procedures on at least an annual basis.

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

DigiCert makes regular system backups on at least a weekly basis and maintains backup copies of its Private Keys, which are stored in a secure, off-site location. If DigiCert discovers that any of its computing resources, software, or data operations have been compromised, DigiCert assesses the threats and risks that the compromise presents to the integrity or security of its operations or those of affected parties. If DigiCert determines that a continued operation could pose a significant risk to Relying Parties or Subscribers, DigiCert suspends such operation until it determines that the risk is mitigated.

5.7.3. Entity Private Key Compromise Procedures

If DigiCert suspects that one of its Private Keys has been comprised or lost then an emergency response team will convene and assess the situation to determine the degree and scope of the incident and take appropriate action. Specifically, DigiCert will:

1. Collect information related to the incident;
2. Begin investigating the incident and determine the degree and scope of the compromise;
3. Have its incident response team determine and report on the course of action or strategy that should be taken to correct the problem and prevent reoccurrence;
4. If appropriate, contact government agencies, law enforcement, and other interested parties and activate any other appropriate additional security measures;
5. If the compromise involves a Private Key used to sign time-stamp tokens, provide a description of the compromise to Subscribers and Relying Parties;
6. Notify any cross-certified entities of the compromise so that they can revoke their cross-Certificates;
7. Make information available that can be used to identify which Certificates and time-stamp tokens are affected, unless doing so would breach the privacy of a DigiCert user or the security of DigiCert's services;
8. Monitor its system, continue its investigation, ensure that data is still being recorded as evidence, and make a forensic copy of data collected;
9. Isolate, contain, and stabilize its systems, applying any short-term fixes needed to return the system to a normal operating state;
10. Prepare and circulate an incident report that analyzes the cause of the incident and documents the lessons learned; and
11. Incorporate lessons learned into the implementation of long term solutions and the Incident Response Plan.

DigiCert may generate a new Key Pair and sign a new Certificate. If a disaster physically damages DigiCert's equipment and destroys all copies of DigiCert's signature keys then DigiCert will provide notice to affected parties at the earliest feasible time.

5.7.4. Business Continuity Capabilities after a Disaster

To maintain the integrity of its services, DigiCert implements data backup and recovery procedures as part of its Business Continuity Management Plan (BCMP). Stated goals of the BCMP are to ensure that certificate status services be only minimally affected by any disaster involving DigiCert's primary facility and that DigiCert be capable of maintaining other services or resuming them as quickly as possible following a disaster. DigiCert reviews, tests, and updates the BCMP and supporting procedures at least annually.

DigiCert's systems are redundantly configured at its primary facility and are mirrored at a separate, geographically diverse location for failover in the event of a disaster. If a disaster causes DigiCert's primary CA or TSA operations to become inoperative, DigiCert will re-initiate its operations at its secondary location giving priority to the provision of certificate status information and time stamping capabilities, if affected.

5.8. CA OR RA TERMINATION

Before terminating its CA or TSA activities, DigiCert will:

1. Provide notice and information about the termination by sending notice by email to its customers, Application Software Vendors, and cross-certifying entities and by posting such information on DigiCert's web site; and
2. Transfer all responsibilities to a qualified successor entity.

If a qualified successor entity does not exist, DigiCert will:

1. transfer those functions capable of being transferred to a reliable third party and arrange to preserve all relevant records with a reliable third party or a government, regulatory, or legal body with appropriate authority;
2. revoke all Certificates that are still un-revoked or un-expired on a date as specified in the notice and publish final CRLs;
3. destroy all Private Keys; and
4. make other necessary arrangements that are in accordance with this CPS.

DigiCert has made arrangements to cover the costs associated with fulfilling these requirements in case DigiCert becomes bankrupt or is unable to cover the costs. Any requirements of this section that are varied by contract apply only the contracting parties.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

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

DigiCert's CA Key Pairs are generated by multiple trusted individuals acting in trusted roles and using a cryptographic hardware device as part of scripted key generation ceremony. The cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. Activation of the hardware requires the use of two-factor authentication tokens. DigiCert creates auditable evidence during the key generation process to prove that the CPS was followed and role separation was enforced during the key generation process. DigiCert requires that an external auditor witness the generation of any CA keys to be used as publicly trusted root Certificates or to sign EV Certificates. For other CA key pair generation ceremonies, an Internal Auditor, external auditor, or independent third party attends the ceremony, or an external auditor examines the signed and documented record of the key generation ceremony, as allowed by applicable policy.

Subscribers must generate their keys in a manner that is appropriate for the certificate type. Certificates issued at Level 3 Hardware or at Level 4 Biometric must be generated on validated hardware cryptographic modules using a FIPS-approved method. Subscribers who generate their own keys for a Qualified Certificate on an SSCD shall ensure that the SSCD meets the requirements of CWA 14169 and that the Public Key to be certified is from the Key Pair generated by the SSCD. For Adobe Signing Certificates, Subscribers must generate their Key Pairs in a medium that prevents exportation or duplication and that meets or exceeds FIPS 140-1 Level 2 certification standards.

6.1.2. Private Key Delivery to Subscriber

If DigiCert, a CMS, or an RA generates a key for a Subscriber, then it must deliver the Private Key securely to the Subscriber. Keys may be delivered electronically (such as through secure email or stored in a cloud-based system) or on a hardware cryptographic module / SSCD. In all cases:

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

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

6.1.3. Public Key Delivery to Certificate Issuer

Subscribers generate Key Pairs and submit the Public Key to DigiCert in a CSR as part of the certificate request process. The Subscriber's signature on the request is authenticated prior to issuing the Certificate.

6.1.4. CA Public Key Delivery to Relying Parties

DigiCert's Public Keys are provided to Relying Parties as specified in a certificate validation or path discovery policy file, as trust anchors in commercial browsers and operating system root store, and/or as roots signed by other CAs. All accreditation authorities supporting DigiCert Certificates and all application software providers are permitted to redistribute DigiCert's root anchors.

DigiCert may also 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. Relying Parties may obtain DigiCert's self-signed CA Certificates from DigiCert's web site or by email.

6.1.5. Key Sizes

DigiCert generally follows the NIST timelines in using and retiring signature algorithms and key sizes. Accordingly, DigiCert is phasing out its use of the SHA-1 hash algorithm. Currently, DigiCert generates and uses at least the following minimum key sizes, signature algorithms, and hash algorithms for signing Certificates, CRLs, and certificate status server responses for policy OIDs of 2.16.840.1.114412.1.11, 2.16.840.1.114412.1.12, or within the policy OID arc of 2.16.840.1.114412.4 (for FBCA Certificates):

2048-bit RSA Key or
384-bit ECDSA Key with Secure Hash Algorithm version 2 (SHA-256) or a hash algorithm that is equally or more resistant to a collision attack). Certificates that do not assert these certificate policies (see other policies listed in Section 1.2) may also be signed using the SHA-1 hash algorithm, provided that its use

otherwise complies with requirements of the CA/Browser Forum or the relevant CP. Signatures on CRLs, OCSP responses, and OCSP responder Certificates that provide status information for Certificates that were generated using SHA-1 may continue to be generated using the SHA-1 algorithm. All other signatures on CRLs, OCSP responses, and OCSP responder Certificates must use the SHA-256 hash algorithm or one that is equally or more resistant to collision attack.

DigiCert requires end-entity Certificates to contain a key size that is at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms.

DigiCert may require higher bit keys in its sole discretion. PIV-I Certificates contain Public Keys and algorithms that conform to [NIST SP 800-78].

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

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

6.1.6. Public Key Parameters Generation and Quality Checking

DigiCert uses a cryptomodule that conforms to FIPS 186-2 and provides random number generation and on-board generation of up to 4096-bit RSA Public Keys and a wide range of ECC curves.

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

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

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

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

Key usage bits and extended key usages are specified in the certificate profile for each type of Certificate as set forth in DigiCert's Certificate Profiles document. DigiCert's CA Certificates have at least two key usage bits set: keyCertSign and cRLSign, and for signing OCSP responses, the digitalSignature bit is also set.

Except for legacy applications requiring a single key for dual use with both encryption and signature, DigiCert does not issue Certificates with key usage for both signing and encryption. Instead, DigiCert issues Subscribers two Key Pairs—one for key management and one for digital signature and authentication. For Certificates at Levels 1, 2 and 3 that are used for signing and encryption in support of legacy applications, they must:

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

No Level 4 Certificates may have such dual-use Key Pairs.
PIV-I Content Signing Certificates also include an extended key usage of id-fpki-pivi-content-signing.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

DigiCert's cryptographic modules for all of its CA and OCSP responder Key Pairs are validated to the FIPS 140 Level 3 and International Common Criteria (CC) Information Technology Security Evaluation Assurance Level (EAL) 14169 EAL 4+ Type 3 (EAL 4 Augmented by AVA_VLA.4 and AVA_MSU.3) in the European Union (EU). IGTF Certificate Subscribers must protect their Private Keys in accordance with the applicable Guidelines on Private Key Protection, including the use of strong pass phrases to protect Private Keys.

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

Assurance Level	Subscriber	Registration Authority
EV Code Signing	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Adobe Signing	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 3 (Hardware)
Rudimentary	N/A	FIPS 140 Level 1 (Hardware or Software)
Basic, LOA2, and LOA3	FIPS 140 Level 1 (Hardware or Software)	FIPS 140 Level 1 (Hardware or Software)
Medium	FIPS 140 Level 1 (Software) FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
Medium Hardware, Biometric & PIV-I Card/Hardware Authentication	FIPS 140 Level 2 (Hardware)	FIPS 140 Level 2 (Hardware)
EU QC on SSCD	EAL 4 Augmented (Hardware)	EAL 4 Augmented (Hardware)

DigiCert ensures that the Private Key of an EV Code Signing Certificate is properly generated, used, and stored in a cryptomodule that meets or exceeds the requirements of FIPS 140 level 2 by (i) shipping conforming cryptomodules with preinstalled Key Pairs, (ii) communicating via PKCS#11 crypto APIs of cryptomodules that DigiCert has verified meet or exceed requirements, or (iii) obtaining an IT audit from the Subscriber that indicates compliance with FIPS 140-2 level 2 or the equivalent.

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

DigiCert's authentication mechanisms are protected securely when not in use and may only be accessed by actions of multiple trusted persons.

Backups of CA Private Keys are securely stored off-site and require two-person access. Re-activation of a backed-up CA Private Key (unwrapping) requires the same security and multi-person control as when performing other sensitive CA Private Key operations.

6.2.3. Private Key Escrow

DigiCert does not escrow its signature keys. Subscribers may not escrow their private signature keys. DigiCert may provide escrow services for other types of Certificates in order to provide key recovery as described in section 4.12.1.

6.2.4. Private Key Backup

DigiCert's Private Keys are generated and stored inside DigiCert's cryptographic module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+. When keys are transferred to other media for backup and disaster recovery purposes, the keys are transferred and stored in an encrypted form. DigiCert's CA Key Pairs are backed up by multiple trusted individuals using a cryptographic hardware device as part of scripted and video-recorded key backup process.

DigiCert may provide backup services for Private Keys that are not required to be kept on a hardware device. Access to back up Certificates is protected in a manner that only the Subscriber can control the Private Key. DigiCert may require backup of PIV-I Content Signing private signature keys to facilitate disaster recovery, provided that all backup is performed under multi-person control. Backed up keys are never stored in a plain text form outside of the cryptographic module.

6.2.5. Private Key Archival

DigiCert does not archive Private Keys.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module. Private Keys are exported from the cryptographic module into backup tokens only for HSM transfer, offline storage, and backup purposes. The Private Keys are encrypted when transferred out of the module and never exist in plaintext form. When transported between cryptographic modules, DigiCert encrypts the Private Key and protects the keys used for encryption from disclosure. Private Keys used to encrypt backups are securely stored and require two-person access.

6.2.7. Private Key Storage on Cryptographic Module

DigiCert's Private Keys are generated and stored inside DigiCert's cryptographic module, which has been evaluated to at least FIPS 140 Level 3 and EAL 4+. Root Private Keys are stored offline in cryptographic modules or backup tokens as described above in Sections 6.2.2, 6.2.4, and 6.2.6.

6.2.8. Method of Activating Private Keys

DigiCert's Private Keys are activated according to the specifications of the cryptographic module manufacturer. Activation data entry is protected from disclosure.

Subscribers are solely responsible for protecting their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their Private Keys. *See also* Section 6.4.

6.2.9. Method of Deactivating Private Keys

DigiCert's Private Keys are deactivated via logout procedures on the applicable HSM device when not in use. Root Private Keys are further deactivated by removing them entirely from the storage partition on the HSM device. 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.

6.2.10. Method of Destroying Private Keys

DigiCert personnel, acting in trusted roles, destroy CA, RA, and status server Private Keys when no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed.

DigiCert may destroy a Private Key by deleting it from all known storage partitions. DigiCert also zeroizes the HSM device and associated backup tokens according to the specifications of the hardware manufacturer. This reinitializes the device and overwrites the data with binary zeros. If the zeroization or re-initialization procedure fails, DigiCert will crush, shred, and/or incinerate the device in a manner that destroys the ability to extract any Private Key.

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

DigiCert archives copies of Public Keys in accordance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

DigiCert Certificates have maximum validity periods of:

Type	**Private Key Use**	**Certificate Term**
Root CA	20 years	25 years
Sub CA*	12 years	15 years
FBCA-Cross-certified Sub CAs	6 years (period of key use for signing Certificates)	10 years (key still signs CRLs, OCSP responses, and OCSP responder Certificates)
IGTF Cross-certified Sub CA*	6 years	15 years
CRL and OCSP responder signing	3 years	31 days†
OV SSL	No stipulation	39 months
EV SSL	No stipulation	27 months
Time Stamping Authority	15 months	135 months
Object Signing Certificate and Document Signing	No stipulation‡	123 months
Code Signing Certificate issued to Subscriber under the Minimum Requirements for Code Signing Certificates or the EV Code Signing Guidelines	No stipulation	39 months
EV Code Signing Certificate issued to Signing Authority	123 months	123 months
Adobe Signing Certificate	39 months	5 years
FBCA and IGTF End Entity Client used for signatures, including EU Qualified Certificates	36 months	36 months
FBCA and IGTF Client used for key management.	36 months	36 months
End Entity Client for all other purposes (FBCA or IGTF compliant)	36 months	36 months
End Entity / Client for all other purposes (non-FBCA and non-IGTF certs)	No Stipulation	60 months
PIV-I Content Signing**	36 months	9 years
PIV-I Cards	6 years	6 years
IGTF on hardware	60 months	13 months
Hotspot 2.0 OSU Server Certificates	No stipulation	2 years

* IGTF signing Certificates have a lifetime that is at least twice the maximum lifetime of an end entity Certificate.
† OCSP responder and CRL signing Certificates associated with a PIV-I Certificate only have a maximum certificate validity period of 31 days.

‡ Code and content signers cross-certified with FBCA may use their Private Keys for three years; the lifetime of the associated Public Keys shall not exceed eight years.
** Subscriber Public Keys in Certificates that assert the PIV-I Content Signing OID in the extended key usage extension have a maximum usage period of nine years. The Private Keys corresponding to the Public Keys in these Certificates have a maximum usage period of three years. Expiration of PIV-I Content Signing Certificate shall be later than the expiration of the PIV-I Hardware and PIV-I Card Authentication Certificates.

Relying parties may still validate signatures generated with these keys after expiration of the Certificate. Private Keys associated with self-signed root Certificates that are distributed as trust anchors are used for a maximum of 20 years. DigiCert does not issue PIV-I subscriber Certificates that expire later than the expiration date of the PIV-I hardware token on which the Certificates reside.

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

6.4. ACTIVATION DATA

6.4.1. Activation Data Generation and Installation

DigiCert activates the cryptographic module containing its CA Private Keys according to the specifications of the hardware manufacturer. This method has been evaluated as meeting the requirements of FIPS 140-2 Level 3. The cryptographic hardware is held under two-person control as explained in Section 5.2.2 and elsewhere in this CPS. DigiCert will only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

All DigiCert personnel and Subscribers are instructed to use strong passwords and to protect PINs and passwords. DigiCert employees are required to create non-dictionary, alphanumeric passwords with a minimum length and to change their passwords on a regular basis. If DigiCert uses passwords as activation data for a signing key, DigiCert will change the activation data change upon rekey of the CA Certificate.

6.4.2. Activation Data Protection

DigiCert protects data used to unlock Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms. Protection mechanisms include keeping activation mechanisms secure using role-based physical control. All DigiCert personnel are instructed to memorize and not to write down their password or share it with another individual. DigiCert locks accounts used to access secure CA processes if a certain number of failed password attempts occur.

6.4.3. Other Aspects of Activation Data

If DigiCert must reset activation data associated with a PIV-I Certificate then DigiCert or an RA performs a successful biometric 1:1 match of the applicant against the biometrics collected in Section 3.2.3.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

DigiCert secures its CA systems and authenticates and protects communications between its systems and trusted roles. DigiCert's CA servers and support-and-vetting workstations run on trustworthy systems that are configured and hardened using industry best practices. All CA systems are scanned for malicious code and protected against spyware and viruses.

DigiCert's CA systems, including any remote workstations, are configured to:

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

All Certificate Status Servers:

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

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

DigiCert has mechanisms in place to control and monitor the acquisition and development of its CA systems. Change requests require the approval of at least one administrator who is different from the person submitting the request. DigiCert only installs software on CA systems if the software is part of the CA's operation. CA hardware and software are dedicated to performing operations of the CA.

Vendors are selected based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. Management is involved in the vendor selection and purchase decision process. Non-PKI hardware and software is purchased without identifying the purpose for which the component will be used. All hardware and software are shipped under standard conditions to ensure delivery of the component directly to a trusted employee who ensures that the equipment is installed without opportunity for tampering.

Some of the PKI software components used by DigiCert are developed in-house or by consultants using standard software development methodologies. All such software is designed and developed in a controlled environment and subjected to quality assurance review. Other software is purchased commercial off-the-shelf (COTS). Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

Updates of equipment and software are purchased or developed in the same manner as the original equipment or software and are installed and tested by trusted and trained personnel. All hardware and software essential to DigiCert's operations is scanned for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

DigiCert has mechanisms in place to control and monitor the security-related configurations of its CA systems. When loading software onto a CA system, DigiCert verifies that the software is the correct version and is supplied by the vendor free of any modifications. DigiCert verifies the integrity of software used with its CA processes at least once a week.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

DigiCert documents and controls the configuration of its systems, including any upgrades or modifications made. DigiCert's CA system is connected to one internal network and is protected by firewalls and Network

Address Translation for all internal IP addresses (e.g., 192.168.x.x). DigiCert's customer support and vetting workstations are also protected by firewall(s) and only use internal IP addresses. Root Keys are kept offline and brought online only when necessary to sign Certificate-issuing subordinate CAs, OCSP Responder Certificates, or periodic CRLs. Firewalls and boundary control devices are configured to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of PKI services by such systems.

DigiCert's security policy is to block all ports and protocols and open only ports necessary to enable CA functions. All CA equipment is configured with a minimum number of services and all unused network ports and services are disabled. DigiCert's network configuration is available for review on-site by its auditors and consultants under an appropriate non-disclosure agreement.

6.8. TIME-STAMPING

The system time on DigiCert's computers is updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to a real time value distributed by a UTC(k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body. DigiCert maintains an internal NTP server that synchronizes with cellular telephone networks and maintains the accuracy of its clock within one second or less. For each timestamp request the internal NTP server is queried for the current time. However, Relying Parties should be aware that all times included in a time-stamp token are synchronized with UTC within the accuracy defined in the time-stamp token itself, if present.

DigiCert will not issue a time-stamp token using any clock that is detected as inaccurate. All clocks used for time-stamping are housed in the DigiCert's secure facilities and are protected against threats that could result in an unexpected change to the clock's time. DigiCert's facilities automatically detect and report any clock that drifts or jumps out of synchronization with UTC. Clock adjustments are auditable events.

Some aspects of RFC 3161 time stamps differ from Microsoft Authenticode time stamps. For RFC 3161-compliant timestamps, DigiCert includes a unique integer for each newly generated time-stamp token. DigiCert only time-stamps hash representations of data, not the data itself. Information can be hashed for time-stamping using SHA-1 or SHA-256 with RSA encryption and either 1024 or 2048 bit key size for signature creation. (SHA-1, SHA-256, SHA-384, SHA-512, MD5, MD4, and MD2 are supported for RFC 3161-based requests.) DigiCert does not examine the imprint being time-stamped other than to check the imprint's length. DigiCert also does not include any identification of the Time Stamp Token Requester (TST Requester) in the time-stamp token. All time-stamp tokens are signed using a key generated exclusively for that purposes and have the property of the key indicated in the Certificate.

TST Requesters request time-stamp tokens by sending a request to DigiCert. After the TST Requester receives a response from DigiCert, it must verify the status error returned in the response. If an error was not returned, the TST Requester must then verify the fields contained in the time-stamp token and the validity of the time-stamp token's digital signature. In particular, the TST Requester must verify that the time-stamped data corresponds to what was requested and that the time-stamp token contains the correct certificate identifier, the correct data imprint, and the correct hash algorithm OID. The TST Requester must also verify the timeliness of the response by verifying the response against a local trusted time reference. The TST Requester is required to notify DigiCert immediately if any information cannot be verified.

Time Stamp Verifiers shall verify the digital signature on the time-stamp token and confirm that the data corresponds to the hash value in the time-stamp token.

6.9. PIV-I CARDS

The following requirements apply to PIV-I Cards:

1. To ensure interoperability with Federal systems, PIV-I Cards use a smart card platform that is on GSA's FIPS 201 Evaluation Program Approved Product List (APL) and use the PIV application identifier (AID).
2. All PIV-I Cards conform to [NIST SP 800-731].

3. The mandatory X.509 Certificate for Authentication is only issued under a policy that is cross certified with the FBCA PIV-I Hardware policy OID.
4. PIV-I Certificates conform to the PIV-I Profile.
5. An asymmetric X.509 Certificate for Card Authentication is included in each PIV-I card. The Certificate:
    a. conforms to PIV-I Profile,
    b. conforms to [NIST SP 800-73], and
    c. is issued under the PIV-I Card Authentication policy.
6. The CMS includes an electronic representation (as specified in SP 800-73 and SP 800-76) of the cardholder's facial image in each PIV-I card.
7. The X.509 Certificates for Digital Signature and Key Management described in [NIST SP 800-73] are optional for PIV-I Cards.
8. The CMS makes its PIV-I Cards visually distinct from a Federal PIV Card to prevent creation of a fraudulent Federal PIV Card. At a minimum, the CMS does not allowed images or logos on a PIV-I Card to be placed within Zone 11, *Agency Seal*, as defined by [FIPS 201].
9. The CMS requires the following items on the front of a card:
    a. Cardholder facial image,
    b. Cardholder full name,
    c. Organizational Affiliation, if exists; otherwise the issuer of the card, and
    d. Card expiration date.
10. PIV-I cards are issued with an expiration date that is six years or less.
11. All PIV-I Cards expire later than the PIV-I Content Signing Certificate on the card.
12. A policy OID that has been mapped to the FBCA PIV-I Content Signing policy OID is included in the digital signature Certificate used to sign objects on the PIV-I Card. The PIV-I Content Signing Certificate conforms to the PIV-I Profile.
13. The PIV-I Content Signing Certificate and corresponding Private Key are managed within a trusted Card Management System.
14. At issuance, the PIV-I Card is activated and released to the subscriber only after a successful 1:1 biometric match of the applicant against the biometrics collected in Section 3.2.3.
15. PIV-I Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system performs a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73]. When cards are personalized, card management keys are set to be specific to each PIV-I Card. That is, each PIV-I Card contains a unique card management key. Card management keys meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78].

7. CERTIFICATE, CRL, AND OCSP PROFILES

DigiCert uses the ITU X.509, version 3 standard to construct digital Certificates for use within the DigiCert PKI. DigiCert adds certain certificate extensions to the basic certificate structure for the purposes intended by X.509v3 as per Amendment 1 to ISO/IEC 9594-8, 1995. For PIV-I Certificates, DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards. For Qualified Certificates, DigiCert follows ETSI TS 101 862.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All Certificates are X.509 version 3 Certificates.

7.1.2. Certificate Extensions

See DigiCert's Certificate Profiles document. IGTF Certificates comply with the Grid Certificate Profile as defined by the Open Grid Forum GFD.125.

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

7.1.3. Algorithm Object Identifiers

DigiCert Certificates are signed using one of the following algorithms:

sha-1WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5]
sha256WithRSAEncryption	[iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11]
ecdsa-with-sha384	[iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures (4) ecdsa-with-SHA2 (3) 3]

DigiCert does not currently sign Certificates using RSA with PSS padding. SSL/TLS Server Certificates are not signed with sha-1WithRSAEncryption.

DigiCert and Subscribers may generate Key Pairs using the following:

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

Elliptic curve Public Keys submitted to DigiCert for inclusion in end entity Certificates should all be based on NIST “Suite B” curves. Signature algorithms for PIV-I Certificates are limited to those identified by NIST SP 800-78.

7.1.4. Name Forms

Each Certificate includes a unique serial number that is never reused. Optional subfields in the subject of an SSL Certificate must either contain information verified by DigiCert or be left empty. SSL Certificates cannot contain metadata such as ‘.’, ‘-‘ and ‘ ‘ characters or any other indication that the field is not applicable. DigiCert logically restricts OU fields from containing Subscriber information that has not been verified in accordance with Section 3.

The Distinguished Name for each Certificate type is set forth in DigiCert’s certificate profiles document. The contents of the fields in EV Certificates must meet the requirements in Section 8.1 of the EV Guidelines.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

An object identifier (OID) is a unique number that identifies an object or policy. The OIDs used by DigiCert are listed in Section 1.2 and in DigiCert’s Certificate Profiles document.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

DigiCert includes brief statements in Certificates about the limitations of liability and other terms associated with the use of a Certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

For PIV-I Certificates, DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

7.2.1. Version number(s)

DigiCert issues version 2 CRLs that contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha384 [1 2 840 10045 4 3 3]
Issuer Distinguished Name	DigiCert
thisUpdate	CRL issue date in UTC format
nextUpdate	Date when the next CRL will issue in UTC format.
Revoked Certificates List	List of revoked Certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the Certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optional reason for revocation

7.3. OCSP PROFILE

For PIV-I Certificates, DigiCert follows the FPKIPA's X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards.

7.3.1. Version Number(s)

DigiCert's OCSP responders conform to version 1 of RFC 2560.

7.3.2. OCSP Extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The practices in this CPS are designed to meet or exceed the requirements of generally accepted industry standards, including the latest version of the EV Guidelines and the WebTrust Program for Certification Authorities, ANS X9.79/ISO 21188 PKI Practices and Policy Framework ("CA WebTrust/ISO 21188"). For purposes of interoperation with the U.S. Government, compliance can be determined by reference to any current auditor letter of compliance meeting FPKIPA Audit Requirements.

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

DigiCert receives an annual audit by an independent external auditor to assess DigiCert's compliance with this CPS, any applicable CPs, and the CA WebTrust/ISO 21188 and WebTrust EV Program criteria. The audit covers DigiCert's RA systems, Sub CAs, and OCSP Responders.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

WebTrust auditors must meet the requirements of Section 14.1.14 of the EV Guidelines. Specifically:

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

Certified Internal Auditor (CIA), or have another recognized information security auditing credential. Auditors must be subject to disciplinary action by its licensing body.

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

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

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

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

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

DigiCert's WebTrust auditor does not have a financial interest, business relationship, or course of dealing that could foreseeably create a significant bias for or against DigiCert.

8.4. TOPICS COVERED BY ASSESSMENT

The audit covers DigiCert's business practices disclosure, the integrity of DigiCert's PKI operations, and DigiCert's compliance with the EV Guidelines. The audit verifies that DigiCert is compliant with the CP, this CPS, and any MOA between it and any other PKI.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

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

8.6. COMMUNICATION OF RESULTS

The results of each audit are reported to the DCPA and to any third party entities which are entitled by law, regulation, or agreement to receive a copy of the audit results. On an annual basis, DigiCert submits a report of its audit compliance to various parties, such as Mozilla, the Federal PKI Policy Authority, CA licensing bodies, etc.

8.7. SELF-AUDITS

On at least a quarterly basis, DigiCert performs regular internal audits against a randomly selected sample of at least three percent of the OV and DV SSL Certificates and at least three percent of the EV SSL and EV Code Signing Certificates issued since the last internal audit. Self-audits on SSL and code signing Certificates are performed in accordance with Guidelines adopted by the CA / Browser Forum.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

9.1.1. Certificate Issuance or Renewal Fees

DigiCert charges fees for certificate issuance and renewal. DigiCert may change its fees at any time in accordance with the applicable customer agreement.

9.1.2. Certificate Access Fees

DigiCert may charge a reasonable fee for access to its certificate databases.

9.1.3. Revocation or Status Information Access Fees

DigiCert does not charge a certificate revocation fee or a fee for checking the validity status of an issued Certificate using a CRL. DigiCert may charge a fee for providing certificate status information via OCSP.

9.1.4. Fees for Other Services

No stipulation.

9.1.5. Refund Policy

Subscribers must request refunds, in writing, within 30 days after a Certificate issues. After receiving the refund request, DigiCert may revoke the Certificate and refund the amount paid by the Applicant, minus any applicable application processing fees.

9.2. FINANCIAL RESPONSIBILITY

9.2.1. Insurance Coverage

DigiCert maintains Commercial General Liability insurance with a policy limit of at least $2 million in coverage and Professional Liability/Errors & Omissions insurance with a policy limit of at least $5 million in coverage. Insurance is carried through companies 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

Insurance coverage for end-entities is specified in DigiCert's Relying Party Agreement.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

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

1. Private Keys;
2. Activation data used to access Private Keys or to gain access to the CA system;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by DigiCert as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. 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
Any information not listed as confidential is considered public information. Published Certificate and revocation data is considered public information.

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

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan
DigiCert follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when the disclosure is required by law or when requested by the subject of the personal information.

9.4.2. Information Treated as Private
DigiCert treats all personal information about an individual that is not publicly available in the contents of a Certificate or CRL as private information. DigiCert protects private information using appropriate safeguards and a reasonable degree of care.

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

9.4.4. Responsibility to Protect Private Information
DigiCert employees and contractors are expected to handle personal information in strict confidence and meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information
Personal information obtained from an applicant during the application or identity verification process is considered private information if the information is not included in a Certificate. DigiCert will only use private information after obtaining the subject's consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a Certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process
DigiCert may disclose private information, without notice, if DigiCert believes the disclosure is required by law or regulation.

9.4.7. Other Information Disclosure Circumstances
No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS
DigiCert and/or its business partners own the intellectual property rights in DigiCert's services, including the Certificates, trademarks used in providing the services, and this CPS. "DigiCert" is a registered trademark of DigiCert, Inc.

Certificate and revocation information are the property of DigiCert. DigiCert grants permission to reproduce and distribute Certificates on a non-exclusive and royalty-free basis, provided that they are reproduced and distributed in full. DigiCert does not allow derivative works of its Certificates or products without prior written permission. Private and Public Keys remain the property of the Subscribers who rightfully hold them. All secret shares (distributed elements) of the DigiCert Private Keys are the property of DigiCert.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

Except as expressly stated in this CPS or in a separate agreement with a Subscriber, DigiCert does not make any representations regarding its products or services. DigiCert represents, to the extent specified in this CPS, that:

1. DigiCert complies, in all material aspects, with the CP, this CPS, and all applicable laws and regulations,
2. DigiCert publishes and updates CRLs and OCSP responses on a regular basis,
3. All Certificates issued under this CPS will be verified in accordance with this CPS and meet the minimum requirements found herein and in the Baseline Requirements,
4. DigiCert will maintain a repository of public information on its website, and
5. Information published on a qualified Certificate meets the requirements specified in EU law.

To the extent allowed under EU law, DigiCert:

1. Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information, including name verification for (1) Certificates intended for email and intranet use, (2) Multi-SAN Certificates, and (3) other Certificates issued to individuals and intranets.
2. Is not responsible for information contained in a Certificate except as stated in this CPS,
3. Does not warrant the quality, function, or performance of any software or hardware device, and
4. Is not responsible for failing to comply with this CPS because of circumstances outside of DigiCert's control.

For EV Certificates, DigiCert represents to Subscribers, Subjects, Application Software Vendors that distribute DigiCert's root Certificates, and Relying Parties that use a DigiCert Certificate while the Certificate is valid that DigiCert followed the EV Guidelines when verifying information and issuing EV Certificates.

This representation is limited solely to DigiCert's compliance with the EV Guidelines (e.g., DigiCert may rely on erroneous information provided in an attorney's opinion or accountant's letter that is checked in accordance with the Guidelines).

For PIV Certificates, DigiCert maintains an agreement with Affiliated Organizations that includes obligations related to authorizing affiliation with Subscribers of PIV-I Certificates.

9.6.2. RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to the DigiCert CP and this CPS,
2. Information provided by the RA does not contain any false or misleading information,
3. Translations performed by the RA are an accurate translation of the original information, and
4. All Certificates requested by the RA meet the requirements of this CPS.

DigiCert's agreement with the RA may contain additional representations.

9.6.3. Subscriber Representations and Warranties

Prior to being issued and receiving a Certificate, subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to notify DigiCert and any applicable RA if a change occurs that could affect the status of the Certificate. Subscribers represent to DigiCert, Application Software Vendors, and Relying Parties that, for each Certificate, the Subscriber will:

1. Securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with DigiCert,
3. Confirm the accuracy of the certificate data prior to using the Certificate,
4. Promptly (i) request revocation of a Certificate, cease using it and its associated Private Key, and notify DigiCert if there is any actual or suspected misuse or compromise of the Private Key

associated with the Public Key included in the certificate, and (ii) request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate,

5. Ensure that individuals using Certificates on behalf of an organization have received security training appropriate to the Certificate,
6. Use the Certificate only for authorized and legal purposes, consistent with the certificate purpose, this CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL Certificates on servers accessible at the domain listed in the Certificate and not using code signing Certificates to sign malicious code or any code that is downloaded without a user's consent, and
7. Promptly cease using the Certificate and related Private Key after the Certificate's expiration.

9.6.4. Relying Party Representations and Warranties

Each Relying Party represents that, prior to relying on a DigiCert Certificate, it:

1. Obtained sufficient knowledge on the use of digital Certificates and PKI,
2. Studied the applicable limitations on the usage of Certificates and agrees to DigiCert's limitations on liability related to the use of Certificates,
3. Has read, understands, and agrees to the DigiCert Relying Party Agreement and this CPS,
4. Verified both the DigiCert Certificate and the Certificates in the certificate chain using the relevant CRL or OCSP,
5. Will not use a DigiCert Certificate if the Certificate has expired or been revoked, and
6. Will take all reasonable steps to minimize the risk associated with relying on a digital signature, including only relying on a DigiCert Certificate after considering:
    a) applicable law and the legal requirements for identification of a party, protection of the confidentiality or privacy of information, and enforceability of the transaction;
    b) the intended use of the Certificate as listed in the certificate or this CPS,
    c) the data listed in the Certificate,
    d) the economic value of the transaction or communication,
    e) the potential loss or damage that would be caused by an erroneous identification or a loss of confidentiality or privacy of information in the application, transaction, or communication,
    f) the Relying Party's previous course of dealing with the Subscriber,
    g) the Relying Party's understanding of trade, including experience with computer-based methods of trade, and
    h) any other indicia of reliability or unreliability pertaining to the Subscriber and/or the application, communication, or transaction.

Any unauthorized reliance on a Certificate is at a party's own risk.

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

EXCEPT AS EXPRESSLY STATED IN SECTION 9.6.1, ALL CERTIFICATES AND ANY RELATED SOFTWARE AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". TO THE MAXIMUM EXTENT PERMITTED BY LAW, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY SERVICE OR PRODUCT WILL MEET ANY EXPECTATIONS OR THAT ACCESS TO CERTIFICATES WILL BE TIMELY OR ERROR-FREE. DigiCert does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time. A fiduciary duty is not created simply because an entity uses DigiCert's services.

9.8. LIMITATIONS OF LIABILITY

NOTHING HEREIN LIMITS LIABILTY RELATED TO (I) DEATH OR PERSONAL INJURY RESULTING FROM DIGICERT'S NEGLIGENCE OR (II) FRAUD COMMITTED BY DIGICERT. EXCEPT AS STATED ABOVE, ANY ENTITY USING A DIGICERT CERTIFICATE OR SERVICE WAIVES ALL LIABILITY OF DIGICERT RELATED TO SUCH USE, PROVIDED THAT DIGICERT HAS MATERIALLY COMPLIED WITH THIS CPS IN PROVIDING THE

CERTIFICATE OR SERVICE. DIGICERT'S LIABILITY FOR CERTIFICATES AND SERVICES THAT DO NOT MATERIALLY COMPLY WITH THIS CPS IS LIMITED AS FOLLOWS:

1. NO LIABILITY IF THE DAMAGE OR LOSS RELATES TO A CERTIFICATE OTHER THAN A SSL CERTIFICATE OR CODE SIGNING CERTIFICATE,
2. A MAXIMUM LIABILITY OF $1,000 PER TRANSACTION FOR SSL CERTIFICATES,
3. AN AGGREGATE MAXIMUM LIABILITY OF $10,000 FOR ALL CLAIMS RELATED TO A SINGLE CERTIFICATE OR SERVICE,
4. AND AN AGGREGATE MAXIMUM LIABILITY OF $1 MILLION FOR ALL CLAIMS, REGARDLESS OF THE NUMBER OR SOURCE OF THE CLAIMS.

DIGICERT APPORTIONS PAYMENTS RELATED TO AN AGGREGATE MAXIMUM LIMITATION ON LIABILITY UNDER THIS SECTION TO THE FIRST CLAIMS THAT ACHIEVE FINAL RESOLUTION.

All liability is limited to actual and legally provable damages. DigiCert is not liable for:

1. Any indirect, consequential, special, or punitive damages or any loss of profit, revenue, data, or opportunity, even if DigiCert is aware of the possibility of such damages;
2. Liability related to fraud or willful misconduct of the Applicant;
3. Liability related to use of a Certificate that exceeds the limitations on use, value, or transactions as stated either in the Certificate or this CPS;
4. Liability related to the security, usability, or integrity of products not supplied by DigiCert, including the Subscriber's and Relying Party's hardware; or
5. Liability related to the compromise of a Subscriber's Private Key.

The limitations in this section apply to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of claims of liability, (iii) the extent or nature of the damages, (iv) whether DigiCert failed to follow any provision of this CPS, or (v) whether any provision of this CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CPS are fundamental terms to the use of DigiCert's Certificates and services.

9.9. INDEMNITIES

9.9.1. Indemnification by DigiCert

DigiCert shall indemnify each Application Software Vendor against any claim, damage, or loss suffered by an Application Software Vendor related to an EV Certificate issued by DigiCert, regardless of the cause of action or legal theory involved, except where the claim, damage, or loss suffered by the Application Software Vendor was directly caused by the Application Software Vendor's software displaying either (1) a valid and trustworthy EV Certificate as not valid or trustworthy or (2) displaying as trustworthy (i) an EV Certificate that has expired or (ii) a revoked EV Certificate where the revocation status is available online but the Application Software Vendor's software failed to check or ignored the status.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, each Subscriber shall indemnify DigiCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, this CPS, or applicable law; (iii) the compromise or unauthorized use of a Certificate or Private Key caused by the Subscriber's negligence or intentional acts; or (iv) Subscriber's misuse of the Certificate or Private Key.

9.9.3. Indemnification by Relying Parties

To the extent permitted by law, each Relying Party shall indemnify DigiCert, its partners, and any cross-signed entities, and their respective directors, officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to the Relying Party's (i) breach of the Relying Party Agreement, an End-User License Agreement, this CPS, or applicable law; (ii) unreasonable reliance on a Certificate; or (iii) failure to check the Certificate's status prior to use.

9.10. TERM AND TERMINATION

9.10.1. Term

This CPS and any amendments to the CPS 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 and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

DigiCert will communicate the conditions and effect of this CPS's termination via the DigiCert Repository. The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination. All Subscriber Agreements remain effective until the Certificate is revoked or expired, even if this CPS terminates.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

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

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This CPS is reviewed annually. Amendments are made by posting an updated version of the CPS to the online repository. Controls are in place to reasonably ensure that this CPS is not amended and published without the prior authorization of the DCPA.

9.12.2. Notification Mechanism and Period

DigiCert posts CPS revisions to its website. DigiCert does not guarantee or set a notice-and-comment period and may make changes to this CPS without notice and without changing the version number. Major changes affecting accredited Certificates are announced and approved by the accrediting agency prior to becoming effective. The DCPA is responsible for determining what constitutes a material change of the CPS.

9.12.3. Circumstances under which OID Must Be Changed

The DCPA is solely responsible for determining whether an amendment to the CPS requires an OID change.

9.13. DISPUTE RESOLUTION PROVISIONS

Parties are required to notify DigiCert and attempt to resolve disputes directly with DigiCert before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14. GOVERNING LAW

The national law of the relevant member state governs any dispute involving Qualified Certificates. Except for disputes involving Qualified Certificates, the laws of the state of Utah govern the interpretation, construction, and enforcement of this CPS and all proceedings related to DigiCert's products and services, including tort claims, without regard to any conflicts of law principles. The state of Utah has non-exclusive venue and jurisdiction over any proceedings related to the CPS or any DigiCert product or service.

9.15. COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products. Subject to section 9.4.5's Notice and Consent to Use Private Information contained in Certificates, DigiCert meets the requirements of the European data protection laws and has established 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 contractually obligates each RA to comply with this CPS and applicable industry guidelines. DigiCert also requires each party using its products and services to enter into an agreement that delineates the terms associated with the product or service. If an agreement has provisions that differ from this CPS, then the agreement with that party controls, but solely with respect to that party. Third parties may not rely on or bring action to enforce such agreement.

9.16.2. Assignment

Any entities operating under this CPS may not assign their rights or obligations without the prior written consent of DigiCert. Unless specified otherwise in a contact with a party, DigiCert does not provide notice of assignment.

9.16.3. Severability

If any provision of this CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CPS will remain valid and enforceable. Each provision of this CPS that provides for a limitation of liability, disclaimer of a warranty, or an exclusion of damages is severable and independent of any other provision.

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 any 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.

9.17. OTHER PROVISIONS

No stipulation.

APPENDIX A: SAMPLE OPINION LETTER

[*Date*]

To: DigiCert, Inc.
2801 N. Thanksgiving Way
Suite 500
Lehi, UT 84043
Email: support@digicert.com
Fax: 801-705-0481

Re: Digital Certificate for *[Exact company name of client – see footnote 1]* (“**Client**”)

This firm represents Client, who asked that I, as its [*accountant ,lawyer, solicitors, barrister, advocate, etc.*], attest to the following information solely as related to the Client’s application for a digital certificate.

After reviewing the Client’s records and based on my investigation, my professional opinion is that:

1. Client is a duly formed [*corporation, LLC, etc.*] under the laws of the [*state/province*] of [*name of governing jurisdiction where Client is incorporated or registered*]; is “active,” “valid,” “current,” or the equivalent; and is not under any known legal disability.

2. [*If applicable*] The Romanized transliteration of Client’s formal legal name is: [*Romanized name]*.

3. [*If applicable*] Client conducts business under the [*assumed/DBA/trade*] name of *[assumed name of Client]*. Client has a currently valid registration of the name with the government agency that has jurisdiction over the place of business listed below.

4. The address where [*Client, Client’s parent, or Client’s subsidiary – select one*] conducts business operations is:
[Insert place of business – this should match the address on the certificate application]

5. A main telephone number at Client’s place of business is:
[Insert primary telephone number of business]

6. *[Name of Client’s Representative – see footnote 2]* is an individual (or are individuals) with the authority to act on behalf of Client to:
a) Provide information about the Client contained in the referenced application,
b) Request one or more digital certificates and designate other persons to request digital certificates, and
c) Agree to the contractual obligations contained in DigiCert’s agreements.

7. *[Name and title of Client’s Representative],* who is Client’s *[Title of Client Representative]*, can be contacted at:
Email: *[Email address of Client Representative]*
Phone: *[Phone number of Client Representative]*

8. Client has either operated as a business for three or more years or has an active deposit account held at a bank or other financial institution where funds deposited are payable on demand.

9. Client has the exclusive right to use the following domain name(s) in identifying itself on the Internet and is aware that it has such control:
[Insert domain names]

Although we did not find any exceptions to the above identification procedures, these procedures do not constitute an audit or opinion of Client's application for a digital certificate. We are not expressing an opinion on Client's digital certificate application and have provided this letter solely for the benefit of DigiCert in connection with Client's application for a digital certificate. No other person or entity may rely on this letter without my express written consent. This letter shall not be quoted in whole or in part, used, published or otherwise referred to or relied upon in any manner, including, without limitation, in any financial statement or other document.

Signature: ____
Print Accountant/Attorney Name: ____
Phone Number: ____
Email: ____
Firm Name: ____
Licensed in: ________________________________
License number, if any: _______________________________
Contact information for licensing agency where this accountant's/attorney's license information may be verified: ____

Note 1: This must be the Client’s exact corporate name as registered with the relevant Incorporating Agency in the Client’s Jurisdiction of Incorporation.
Note 2: A Power of Attorney from an officer of the Client who has the power to delegate authority is sufficient to establish the Client Representative’s actual authority. Multiple representatives may be listed.
Note 3: In-house counsel of the Client may submit this letter if permitted by the rules of your jurisdiction.
Note 4: This letter may be submitted by mail, fax, or email.

RELYING PARTY AGREEMENT AND LIMITED WARRANTY

YOU ARE REQUIRED TO READ THIS AGREEMENT CAREFULLY BEFORE RELYING ON A DIGICERT CLICKID SITE SEAL, SSL CERTIFICATE, OR OTHER SITE AUTHENTICATION PRODUCT OR SERVICE. IF YOU DO NOT AGREE TO THE TERMS HEREIN, YOU MAY NOT RELY ON OR USE A DIGICERT SITE AUTHENTICATION PRODUCT OR SERVICE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1-800-896-7973.

This relying party agreement is between DigiCert, Inc., a Utah corporation (**"DigiCert"**) and you, the entity or individual relying on a DigiCert ClickID Site Seal, SSL certificate, or other site authentication product or service. You agree as follows:

1. Definitions

1.1. "Certificate" means an X.509v-3 formatted data structure that is signed by DigiCert.

1.2. "Certificate Chain" means an ordered list of Certificates.

1.3. "CPS" means the written statement of the policies and procedures used to operate DigiCert's PKI infrastructure. The CPS is available at http://www.digicert.com/ssl-cps-repository.htm.

1.4. "Relying Party" shall mean an entity that acts in reliance on the information provided by DigiCert in a Site Seal, Certificate, or other site authentication product or service.

1.5. "Site Seal" means a hyperlinked graphic provided by DigiCert to a Verified Identity for display on the Subject's web site.

1.6. "Subject" means the entity that is listed in a DigiCert product or service as the authorized user of the product or service.

1.7. "Verified Identity" means the identity of the Subject as displayed by or listed in a DigiCert site authentication product or service.

2. Use.

2.1. Applicability. This agreement is effective immediately upon your use of or reliance on a DigiCert site authentication product or service, such as when your SSL-enabled device is presented with a Certificate or when you access a website displaying a DigiCert Site Seal. The agreement lasts for as long as you assert that you have reasonably relied on a DigiCert site authentication product or service.

2.2. Reliance. Subject to the conditions herein, you may rely on DigiCert's products and services for their intended purpose as described on DigiCert's website and in its CPS.

2.3. Limitations on Use**.** You may not rely on a DigiCert site authentication product or service to control equipment in hazardous circumstances, or with any system where a failure could lead to death, personal injury, or severe environmental damage.

3. Limited Warranty

3.1. Limited Warranty. Subject to the limits, requirements, and conditions set forth herein, DigiCert warrants to you that, prior to the Certificate's or Site Seal's issuance, DigiCert verified the Subject's legal existence and determined that the named Subject was an entity that controlled the site identified by the Certificate or Site Seal. This warranty does not apply to Client Certificates, Code Signing Certificates, Intranet Certificates (such as Certificates that do not include a fully-qualified domain name), the transaction of sensitive or private information, or any actions or omissions of a third party, including the Subject. This warranty is void if you breach the terms of this agreement.

3.2. Qualifications. The warranty provided herein only applies if all of the following are true:

(i) Prior to relying on the site authentication product or service, you checked all status information provided by DigiCert related to the site authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCSP information available). For Site Seals, this includes verifying the Site Seal's authorization and validity directly with DigiCert and receiving a clear confirmation that the Subject was and remains authorized to display or use the Site Seal.

(ii) Prior to relying on a site authentication product or service, you gathered sufficient information to make an informed decision about the proper use of the authentication product or service and whether your intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with your intended use and the limitations associated with the site authentication product or service provided by DigiCert.

(iii) Your reliance on the site authentication product or service is reasonable based on the circumstances. Your reliance is not reasonable if (i) there was information reasonably available, or if information was known by or presented to you, that would have led a reasonable person not to conduct business through the site or (ii) you used software or hardware that did not satisfactorily perform the technological procedures required to verify the validity of the relied upon site authentication product or service.

(iv) You relied on the site authentication product or service when conducting an online transaction with the Subject during an SSL/TLS encrypted session and that transaction resulted in a fraudulent charge.

(v) You disputed the unauthorized charge with any applicable service provider in accordance with the conditions and terms of the service provider, but the service provider refused to reverse the transaction, issue a refund, or provide other reimbursement for the unauthorized charge.

(vi) You submit the claim via email to support@digicert.com within 60 days after the transaction occurs. A failure to submit the claim via email within the required 60-day period constitutes a conclusive waiver of the claim. The email claim must include your contact information (name, street address, phone number and e-mail address); the date of loss and a detailed description of the events and circumstances related to the loss; the web site URL and Subject name through which the loss occurred; the amount of the loss; information about the service providers involved in the financial transaction (credit card issuer, bank providing the wire transfer, etc.); and a description of any additional information, logs, records or supporting information that you have.

(vii) You cooperate fully with any investigation of your claim, including providing additional information and granting rights of subrogation, if requested.

3.3. Processing. Within 30 days after receiving your email and all supporting documentation (including a determination from any applicable service provider concerning any reversal, reimbursement, or refund of the charge), DigiCert will determine the amount eligible for reimbursement. If you do not receive a response from DigiCert within 60 days of submitting all supporting documentation, then the claim is deemed denied. If you are not satisfied with DigiCert's initial determination of your claim, then, within 30 days of the denial or partial denial, you must send a notice by certified mail to DigiCert requesting a legal review of your claim. Your failure to send such notice under this mandatory procedure within 30 days after initial denial of the claim constitutes waiver of appeal and DigiCert's initial determination is final, binding, and a complete defense and bar to any attempt at judicial review on the ground of failure to exhaust administrative remedies.

4. Disclaimers and Limitations on Liability

4.1. Warranty Disclaimers. DIGICERT'S SITE AUTHENTICATION PRODUCTS AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". THE USE OF A PRODUCT AND/OR SERVICE IS AT YOUR OWN RISK. EXCEPT FOR THE LIMITED WARRANTY UNDER SECTION 3, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY PRODUCTS OR SERVICES WILL MEET YOUR EXPECTATIONS OR THAT ACCESS TO PRODUCTS OR SERVICES WILL BE TIMELY OR ERROR-FREE. DIGICERT DOES NOT WARRANT ANY THIRD PARTY PRODUCT OR SERVICE, INCLUDING ANY WEBSITE THAT IS SECURED BY A DIGICERT CERTIFICATE OR DISPLAYING A DIGICERT SITE SEAL.

4.2. Limitations on Reimbursement. If DigiCert breaches the warranty made in Section 3.1, if you meet the requirements in Section 3.2, and if you are in compliance with this agreement, then DigiCert will reimburse you for the actual unreimbursed unauthorized charge up to a maximum of the lesser of (i) the amount of the unauthorized charge, (ii) $1,000 U.S. per claim, (iii) $10,000 in aggregate for all transactions conducted by you or, if applicable, your affiliates, and (iv) $1,000,000 aggregate for all Relying Parties ("**Aggregate Limit**"). DigiCert administers all claims on a first-come, first-serve basis. Your reliance on multiple products and services used on the same website are mutually exclusive, (i.e. you may not make a warranty claim for both a Site Seal and Certificate used on the same site or with the same transaction). Payments made to you or another Relying Party by DigiCert will decrease the amount available under the Aggregate Limit to all other Relying Parties. If the Aggregate Limit is met, then you waive DigiCert of any liability for all remaining unreimbursed unauthorized charges, regardless of whether any amount was actually paid to you.

4.3. Limitation on Liability. EXCEPT FOR CLAIMS UNDER SECTION 3 (WHICH ARE SUBJECT TO THE LIMITS SET FORTH IN 4.2), YOU HEREBY WAIVE ALL LIABILITY OF DIGICERT AND ITS OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, CONTRACTORS, AND AGENTS, RESULTING FROM OR CONNECTED TO THE RELIANCE ON OR USE OF DIGICERT'S SITE AUTHENTICATION PRODUCTS AND SERVICES, INCLUDING ANY LOSS RELATED TO THE ACTIONS OR OMISSIONS OF A SUBJECT OR OTHER THIRD PARTY. YOU WAIVE ALL LIABILITY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RELATED TO THIS AGREEMENT OR A DIGICERT PRODUCT OR SERVICE, INCLUDING ALL DAMAGES FOR LOST PROFITS, REVENUE, USE, OR DATA. THIS WAIVER APPLIES EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

4.4. Force Majeure and Internet Frailties. Neither party is liable for any failure or delay in performing its obligations under this agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonably control. You acknowledge that DigiCert's products and services are subject to the operation and telecommunication infrastructures of the Internet and the operation of your Internet connection services, all of which are beyond DigiCert's control.

4.5. Applicability. The waivers and limitations in this section 4 apply only to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of any claims, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this agreement have been breached or proven ineffective.

5. INDEMNIFICATION

5.1. Indemnification. You shall indemnify DigiCert and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns against all liabilities, claims, damages, costs, and expenses, including reasonable attorney's fees, related to (i) your failure to comply with this agreement or (ii) your improper use of, or unreasonable reliance on, a DigiCert product or service.

5.2. Indemnification Procedure. DigiCert shall promptly notify you of any such claim, and you shall bear full responsibility for the defense of such claim (including any settlements), provided that (i) you inform and consult with DigiCert about the progress of any litigation or settlement; (ii) any settlement does not stipulate any liability or wrong-doing by DigiCert, and (iii) any settlement does not requires specific performance by DigiCert. DigiCert may elect to participate in the defense of a claim using counsel of its choice at its own expense.

6. MISCELLANEOUS

6.1. Entire Agreement. This agreement constitutes the entire agreement between the parties with respect to your reliance on DigiCert's products and services, superseding all other agreements that may exist. DigiCert may, without notice, amend this agreement and the conditions under which you may rely on a DigiCert site authentication product or service. Amendments are effective when posted to DigiCert's website. You shall periodically review the website to be aware of any changes.

6.2. Notices. You shall send all notices in English writing by first class mail with return receipt request to DigiCert, Inc., Attn: Legal Department, 2600 West Executive Parkway, Suite 500, Lehi, UT 84043. DigiCert will post notices to you on its website.

6.3. Assignment. You shall not assign any of your rights or obligations under this agreement without the prior written consent of DigiCert. Any transfer without consent is void and a material breach of this agreement. DigiCert may assign its rights and obligations without your consent.

6.4. Dispute Resolution. At least 60 days before filing a suit or initiating an administrative claim, you shall notify DigiCert and any other party to the dispute and attempt to settle the dispute in good-faith via a business discussion.

6.5. Governing Law and Jurisdiction. The laws of the state of Utah govern the interpretation, construction, and enforcement of this agreement and all matters related to it, including tort claims, without regards to any conflicts-of-laws principles. The parties hereby submit to the exclusive jurisdiction of and venue in the state and federal courts located in the State of Utah. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this agreement.

6.6. Severability. The invalidity or unenforceability of a provision under this agreement, as determined by a court or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this agreement. The parties shall substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.

6.7. Rights of Third Parties. No third party has any rights or remedies under this agreement.

6.8. Interpretation. The definitive version of this agreement is written in English. If this agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls. Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

Last updated on 26 June 2013

Relying Party Agreement and Limited Warranty

YOU ARE REQUIRED TO READ THIS AGREEMENT CAREFULLY BEFORE RELYING ON A DIGICERT CLICKID SITE SEAL, SSL CERTIFICATE, OR OTHER SITE AUTHENTICATION PRODUCT OR SERVICE. IF YOU DO NOT AGREE TO THE TERMS HEREIN, YOU MAY NOT RELY ON OR USE A DIGICERT SITE AUTHENTICATION PRODUCT OR SERVICE. IF YOU HAVE ANY QUESTIONS REGARDING THIS AGREEMENT, PLEASE E-MAIL DIGICERT AT LEGAL@DIGICERT.COM OR CALL 1.800.896.7973.

This relying party agreement is between DigiCert, Inc., a Utah corporation ("DigiCert") and you, the entity or individual relying on a DigiCert ClickID Site Seal, SSL certificate, or other site authentication product or service. You agree as follows:

1. DEFINITIONS

1.1. "**Certificate**" means an X.509v-3 formatted data structure that is signed by DigiCert.

1.2. "**Certificate Chain**" means an ordered list of Certificates.

1.3. "**CPS**" means the written statement of the policies and procedures used to operate DigiCert's PKI infrastructure. The CPS is available at http://www.digicert.com/ssl-cps-repository.htm.

1.4. "**Relying Party**" shall mean an entity that acts in reliance on the information provided by DigiCert in a Site Seal, Certificate, or other site authentication product or service.

1.5. "**Site Seal**" means a hyperlinked graphic provided by DigiCert to a Verified Identity for display on the Subject's web site.

1.6. "**Subject**" means the entity that is listed in a DigiCert product or service as the authorized user of the product or service.

1.7. "**Verified Identity**" means the identity of the Subject as displayed by or listed in a DigiCert site authentication product or service.

2. USE

2.1. **Applicability.** This agreement is effective immediately upon your use of or reliance on a DigiCert site authentication product or service, such as when your SSL-enabled device is presented with a Certificate or when you access a website displaying a DigiCert Site Seal. The agreement lasts for as long as you assert that you have reasonably relied on a DigiCert site authentication product or service.

2.2. **Reliance.** Subject to the conditions herein, you may rely on DigiCert's products and services for their intended purpose as described on DigiCert's website and in its CPS.

2.3. **Limitations on Use.** You may not rely on a DigiCert site authentication product or service to control equipment in hazardous circumstances, or with any system where a failure could lead to death, personal injury, or severe environmental damage.

3. LIMITED WARRANTY

3.1. **Limited Warranty**. Subject to the limits, requirements, and conditions set forth herein, DigiCert warrants to you that, prior to the Certificate's or Site Seal's issuance, DigiCert verified the Subject's legal existence and determined that the named Subject was an entity that controlled the site identified by the Certificate or Site Seal. This warranty does not apply to Client Certificates, Code Signing Certificates, Intranet Certificates (such as Certificates that do not include a fullyqualified domain name), the transaction of sensitive or private information, or any actions or omissions of a third party, including the Subject. This warranty is void if you breach the terms of this agreement.

3.2. **Qualifications**. The warranty provided herein only applies if all of the following are true:

(i) Prior to relying on the site authentication product or service, you checked all status information provided by DigiCert related to the site authentication product or service to confirm that the information was still valid and that the product or service had not expired or been revoked. For Certificates, this includes checking to ensure that each Certificate in the Certificate Chain is valid, unexpired, and non-revoked (by using any CRL or OCS information available). For Site Seals, this includes verifying the Site Seal's authorization and validity directly with DigiCert and receiving a clear confirmation that the Subject was and remains authorized to display or use the Site Seal.

(ii) Prior to relying on a site authentication product or service, you gathered sufficient information to make an informed decision about the proper use of the authentication product or service and whether your intended reliance on the authentication product or service was reasonable in light of the circumstances. This includes evaluating the risks associated with your intended use and the limitations associated with the site authentication product or service provided by DigiCert.

(iii) Your reliance on the site authentication product or service is reasonable based on the circumstances. Your reliance is not reasonable if (i) there was information reasonably available, or if information was known by or presented to you, that would have led a reasonable person not to conduct business through the site or (ii) you used software or hardware that did not satisfactorily perform the technological procedures required to verify the validity of the relied upon site authentication product or service.

(iv) You relied on the site authentication product or service when conducting an online transaction with the Subject during an SSL/TLS encrypted session and that transaction resulted in a fraudulent charge.

(v) You disputed the unauthorized charge with any applicable service provider in accordance with the conditions and terms of the service provider, but the service provider refused to reverse the transaction, issue a refund, or provide other reimbursement for the unauthorized charge.

(vi) You submit the claim via email to support@digicert.com within 60 days after the transaction occurs. A failure to submit the claim via email within the required 60-day period constitutes a conclusive waiver of the claim. The email claim must include your contact information (name, street address, phone number and e-mail address); the date of loss and a detailed description of the events and circumstances related to the loss; the web site URL and Subject name through which the loss occurred; the amount of the loss; information about the service providers involved in the financial transaction (credit card issuer, bank providing the wire transfer, etc.); and a description of any additional information, logs, records or supporting information that you have.

(vii) You cooperate fully with any investigation of your claim, including providing additional information and granting rights of subrogation, if requested.

3.3. **Processing**. Within 30 days after receiving your email and all supporting documentation (including a determination from any applicable service provider concerning any reversal, reimbursement, or refund of the charge), DigiCert will determine the amount eligible for reimbursement. If you do not receive a response from DigiCert within 60 days of submitting all supporting documentation, then the claim is deemed denied. If you are not satisfied with DigiCert's initial determination of your claim, then, within 30 days of the denial or partial denial, you must send a notice by certified mail to DigiCert requesting a legal review of your claim. Your failure to send such notice under this mandatory procedure within 30 days after initial denial of the claim constitutes waiver of appeal and DigiCert's initial determination is final, binding, and a complete defense and bar to any attempt at judicial review on the ground of failure to exhaust administrative remedies.

4. DISCLAIMERS AND LIMITATIONS ON LIABILITY

4.1. **Warranty Disclaimers**. DIGICERT'S SITE AUTHENTICATION PRODUCTS AND SERVICES ARE PROVIDED "AS IS" AND "AS AVAILABLE". THE USE OF A PRODUCT AND/OR SERVICE IS AT YOUR OWN RISK. EXCEPT FOR THE LIMITED WARRANTY UNDER SECTION 3, DIGICERT DISCLAIMS ALL EXPRESS AND IMPLIED WARRANTIES, INCLUDING ALL WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT. DIGICERT DOES NOT WARRANT THAT ANY PRODUCTS OR SERVICES WILL MEET YOUR EXPECTATIONS OR THAT ACCESS TO PRODUCTS OR SERVICES WILL BE TIMELY OR ERRORFREE. DIGICERT DOES NOT WARRANT ANY THIRD PARTY PRODUCT OR SERVICE, INCLUDING ANY WEBSITE THAT IS SECURED BY A DIGICERT CERTIFICATE OR DISPLAYING A DIGICERT SITE SEAL.

4.2. **Limitations on Reimbursement**. If DigiCert breaches the warranty made in Section 3.1, if you meet the requirements in Section 3.2, and if you are in compliance with this agreement, then DigiCert will reimburse you for the actual unreimbursed unauthorized charge up to a maximum of the lesser of (i) the amount of the unauthorized charge, (ii) $1,000 U.S. per claim, (iii) $10,000 in aggregate for all transactions conducted by you or, if applicable, your affiliates, and (iv) $1,000,000 aggregate for all Relying Parties ("Aggregate Limit"). DigiCert administers all claims on a first-come, first-serve basis. Your reliance on multiple products and services used on the same website are mutually exclusive, (i.e. you may not make a warranty claim for both a Site Seal and Certificate used on the same site or with the same transaction). Payments made to you or another Relying Party by DigiCert will decrease the amount available under the Aggregate Limit to all other Relying Parties. If the Aggregate Limit is met, then you waive DigiCert of any liability for all remaining unreimbursed unauthorized charges, regardless of whether any amount was actually paid to you.

4.3. **Limitation on Liability.** EXCEPT FOR CLAIMS UNDER SECTION 3 (WHICH ARE SUBJECT TO THE LIMITS SET FORTH IN 4.2), YOU HEREBY WAIVE ALL LIABILITY OF DIGICERT AND ITS OFFICERS, DIRECTORS, PARTNERS, EMPLOYEES, CONTRACTORS, AND AGENTS, RESULTING FROM OR CONNECTED TO THE RELIANCE ON OR USE OF DIGICERT'S SITE AUTHENTICATION PRODUCTS AND SERVICES, INCLUDING ANY LOSS RELATED TO THE ACTIONS OR OMISSIONS OF A SUBJECT OR OTHER THIRD PARTY. YOU WAIVE ALL LIABILITY FOR ANY SPECIAL, INDIRECT, INCIDENTAL, OR CONSEQUENTIAL DAMAGES RELATED TO THIS AGREEMENT OR A DIGICERT PRODUCT OR SERVICE, INCLUDING ALL DAMAGES FOR LOST PROFITS, REVENUE, USE, OR DATA. THIS WAIVER APPLIES EVEN IF DIGICERT IS AWARE OF THE POSSIBILITY OF SUCH DAMAGES.

4.4. **Force Majeure and Internet Frailties.** Neither party is liable for any failure or delay in performing its obligations under this agreement to the extent that the circumstances causing such failure or delay are beyond a party's reasonably control. You acknowledge that DigiCert's products and services are subject to the operation and telecommunication infrastructures of the Internet and the operation of your Internet connection services, all of which are beyond DigiCert's control.

4.5. **Applicability.** The waivers and limitations in this section 4 apply only to the maximum extent permitted by law and apply regardless of (i) the reason for or nature of the liability, including tort claims, (ii) the number of any claims, (iii) the extent or nature of the damages, or (iv) whether any other provisions of this agreement have been breached or proven ineffective.

5. INDEMNIFICATION

5.1. **Indemnification.** You shall indemnify DigiCert and its contractors, agents, employees, officers, directors, shareholders, affiliates, and assigns against all liabilities, claims, damages, costs, and expenses, including reasonable attorney's fees, related to (i) your failure to comply with this agreement or (ii) your improper use of, or unreasonable reliance on, a DigiCert product or service.

5.2. **Indemnification Procedure.** DigiCert shall promptly notify you of any such claim, and you shall bear full responsibility for the defense of such claim (including any settlements), provided that (i) you inform and consult with DigiCert about the progress of any litigation or settlement; (ii) any settlement does not stipulate any liability or wrong-doing by DigiCert, and (iii) any settlement does not requires specific performance by DigiCert. DigiCert may elect to participate in the defense of a claim using counsel of its choice at its own expense.

6. MISCELLANEOUS

6.1. **Entire Agreement.** This agreement constitutes the entire agreement between the parties with respect to your reliance on DigiCert's products and services, superseding all other agreements that may exist. DigiCert may, without notice, amend this agreement and the conditions under which you may rely on a DigiCert site authentication product or service. Amendments are effective when posted to DigiCert's website. You shall periodically review the website to be aware of any changes.

6.2. **Notices.** You shall send all notices in English writing by first class mail with return receipt request to DigiCert, Inc., Attn: Legal Department, 2600 West Executive Parkway, Suite 500, Lehi, UT 84043. DigiCert will post notices to you on its website.

6.3. **Assignment.** You shall not assign any of your rights or obligations under this agreement without the prior written consent of DigiCert. Any transfer without consent is void and a material breach of this agreement. DigiCert may assign its rights and obligations without your consent.

6.4. **Dispute Resolution.** At least 60 days before filing a suit or initiating an administrative claim, you shall notify DigiCert and any other party to the dispute and attempt to settle the dispute in goodfaith via a business discussion.

6.5. **Governing Law and Jurisdiction.** The laws of the state of Utah govern the interpretation, construction, and enforcement of this agreement and all matters related to it, including tort claims, without regards to any conflicts-of-laws principles. The parties hereby submit to the exclusive jurisdiction of and venue in the state and federal courts located in the State of Utah. The United Nations Convention on Contracts for the International Sale of Goods does not apply to this agreement.

6.6. **Severability.** The invalidity or unenforceability of a provision under this agreement, as determined by a court or administrative body of competent jurisdiction, does not affect the validity or enforceability of the remainder of this agreement. The parties shall substitute any invalid or unenforceable provision with a valid or enforceable provision that achieves the same economic, legal, and commercial objectives as the invalid or unenforceable provision.

6.7. **Rights of Third Parties.** No third party has any rights or remedies under this agreement.

6.8. **Interpretation.** The definitive version of this agreement is written in English. If this agreement is translated into another language and there is a conflict between the English version and the translated version, the English language version controls. Section headings are for reference and convenience only and are not part of the interpretation of this agreement.

Last updated on 26 June 2013

DigiCert, Inc. Trademark Usage Guidelines

INTRODUCTION

This document (the "Policy") outlines DigiCert's policies regarding any person's or entity's ("User") use of trademarks, logos, and site seals ("Trademarks" or a "Trademark") owned by DigiCert, Inc., a Utah corporation ("DigiCert"). The purpose of this document is to ensure that the Trademarks remain strong and continue to serve as source and quality indicators of DigiCert's products and services while permitting DigiCert's partners and customers to accurately describe their affiliation with DigiCert. Examples of Trademarks include DigiCert®, CertCentral®, ClickID®, Wildcard Plus®, Direct Cert Portal®, Certificate Inspector®, DirectAssured®, and any logos or site seals created or distributed by DigiCert. This list is not exclusive and does not limit the scope of what DigiCert claims as protected material.

GENERAL GUIDELINES

DigiCert encourages its partners and customers to use the Trademarks in publicly distributed materials that reference DigiCert's products and services. However, the Trademarks must be used in accordance with this Policy and may not be displayed:

- in a manner that could confuse a viewer about the source of a product or service, including using a Trademark to falsely imply that DigiCert endorses a non-DigiCert product or service,
- in material that disparages DigiCert,
- for purely decorative purposes, or
- in material that DigiCert finds objectionable.

Use of a Trademark in accordance with this Policy does not require additional approval. Other uses, whether commercial or non-commercial, require DigiCert's prior written permission. Any use not contemplated in this Policy, or not approved in writing, is unauthorized and violates DigiCert's rights.

PERMITTED USERS

Only a User that has a contractual relationship with DigiCert is permitted to use a Trademark in connection with the User's website. A User's license to use a Trademark is expressly granted in the applicable agreement with DigiCert. Anyone may use a DigiCert text Trademark to make true and factual statements about the products bearing the mark.

EXCLUSIVE OWNERSHIP OF THE TRADEMARKS

DigiCert is the exclusive owner of the Trademarks and is the only entity entitled to register or claim an ownership interest in a Trademark or a derivative work of a Trademark. Users may not (i) incorporate a Trademark into their product or service names, company or trade names, marks, logos, internet domain names, or social media profiles, (ii) use the Trademark in a manner that is misleading, fraudulent, or likely to cause confusion or mistake, or (iii) attempt to register a trademark or domain name that contains or is a derivative of a Trademark.

ATTRIBUTION OF OWNERSHIP

Material displaying a Trademark must attribute ownership of the Trademark to DigiCert. The material must not display the Trademark more prominently than User's own logos and trademarks. Material displaying a Trademark should include the following statement: “___ _ [is a/are] trademark[s] of DigiCert, Inc. and [is/are]protected under the laws of the United States and possibly other countries.” The blank space should list all Trademarks used in the material, and the inapplicable text in the brackets should be deleted along with the brackets.

Trademarks must include the proper registration notation (® for registered trademarks and ™ for non-registered trademarks). In text, only the first instance of the Trademark needs annotation. After the first instance, dropping the ® or ™ is permitted. For logos, include the ® or ™ in each instance.

When using a Trademark on a website or on another Internet-enabled medium, at least one reference to DigiCert must include a link to www.digicert.com.

SPECIAL RULES FOR DISPLAYING LOGOS AND SITE SEALS

Users must treat DigiCert’s logos and site seals as a single piece of art, not as a conglomeration of text. Logos and site seals must be produced in the highest quality available. Resized logos and site seals must retain their original proportions and must never be so small that the letters and shape of the Trademark are unrecognizable. Users must surround logos and site seals with a clear area that is free from lettering or design elements. Derivative works— the modifying of logos and site seals (other than resizing)— are not permitted.

GRAMMAR RULES FOR UTILIZING TRADEMARKS

Trademarks must be used as adjectives followed by a generic modifier and not as nouns, verbs, or in the plural form. For example:

Correct: DigiCert® certificates are incredible.

Incorrect: DigiCerts are incredible.

Because Trademarks are not nouns they must not be used in the possessive form, unless the Trademark itself is in possessive form. For example:

Correct: They enhanced the features of CertCentral® certificate management.

Incorrect: They enhanced CertCentral’s features.

Users may not vary the appearance of trademarks by abbreviating them, incorporating them into acronyms, changing their spelling, or improperly capitalizing them.

USAGE RULES FOR DIGICERT AS A TRADE NAME

“DigiCert” functions not only as a trademark that identifies DigiCert as the source of goods and services it offers but also as a trade name referring to DigiCert, Inc. Trade names are nouns and therefore, must not be followed by a generic descriptor but may be used in the possessive form.

In text format, the first reference to the trade or company name must be “DigiCert, Inc”. “DigiCert” can be used for subsequent trade name references. When used as a trade name, “DigiCert” should not be followed by a trademark symbol.

LINKING

Linking to DigiCert's website is permitted. Trademarks that include a link must both follow this Policy and point to the official DigiCert website.

TRADEMARK ABUSE

Trademark misuse should be reported to legal@digicert.com. Please provide all information relevant to the misuse, including where the misuse occurred.

DigiCert reserves the right to review any use of its Trademarks and may object to any use that it deems a violation of this Policy. User agrees to promptly cease using a Trademark if DigiCert objects to its use.

AMENDMENTS

DIGICERT MAY MODIFY ITS TRADEMARKS AND THIS POLICY AT ANY TIME. PLEASE REFER TO THIS POLICY REGULARLY TO ENSURE COMPLIANCE. This Policy was last updated on April 3, 2017.

QUESTIONS

If you have any questions about this Policy, please contact legal@digicert.com.

Introduction

Several *Cerner Millennium* solutions have been Direct-enabled including *PowerChart* Message Center, Remote Report Distribution, Clinical Reporting XR, Cerner Patient Portal, and Health Maintenance Invitations. Every one of those solutions use the same core foreign system interface (FSI) services to communicate with the Cerner Direct HISP.

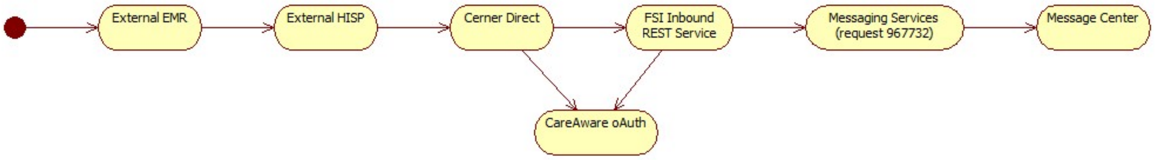
The primary FSI services are FSI Message Interoperability (SCP 504) and FSI Direct Messaging EAR (Enterprise Appliance). They have dependencies related to OAuth and Enterprise Appliance.

The following diagrams from All About Message Center Secure Messaging use *PowerChart* Message Center as the front-end solution to illustrate the message flow through the FSI services. It is important to note there are two different and unrelated OAuth Providers referenced in the diagrams:

- OAuth Cloud in the outbound flow refers to the Cerner Central OAuth Provider. This OAuth Provider protects the services hosted by Cerner Direct.
- CareAware OAuth in the inbound flow refers to Millennium OAuth. This OAuth Provider is a *Cerner Millennium* service that protects services hosted within your *Cerner Millennium* environment. In this case, it protects the FSI Direct Messaging service.

Outbound Flow:

Inbound Flow:



Licensing Requirements

The following licenses are required to use Cerner Direct HISP with *Cerner Millennium* for Meaningful Use Stage 2 attestation:

- Cerner Direct HISP Connection
- *CareAware MultiMedia* Archive

System Requirements

- **Minimum Code Level 2012.01.16**
  - Specific packages that are required are listed in the Release Considerations box on the All About Secure Messaging page. Note that these are the minimum packages required. You can have the minimum packages listed or any package that has replaced these.
- **Prerequisites for Cerner Direct Build:**
  - CareAware MultiMedia Archive
  - In order to send CCDs outbound, the Clinical Document Generator build (in other words, CCD template build) must be complete.
- **Hardware Requirements:**
  - Enterprise Appliance (WAS capacity required is four JVMs for non-prod and four for production).

- **Domain Strategy**

  - Direct build will occur in one non-production domain per prod domain. The same non-production domain should be used for the duration of the project. No non-prod switches, refreshes or code freezes should be scheduled during the project.

Cerner Direct

Cerner Direct Privacy Policy

Overview

Cerner Corporation ("Cerner") is committed to protecting the privacy and security of the personal information that you entrust to us. This privacy policy (the "Privacy Policy") describes how Cerner protects the privacy and security of your personal information. Your use of *Cerner Direct* is governed by the terms of this Privacy Policy. If you do not agree to this Privacy Policy, you may not use *Cerner Direct*. Additional terms and conditions, if any, regarding the collection and use of your information may also be provided to you before you sign up for a particular program or service.

Cerner Direct's Privacy Principles

- The only personal information *Cerner Direct* obtains about you is that which you supply voluntarily. In cases when *Cerner Direct* may need personal information to provide you with customized content or to inform you about new features or services, you will be asked for that information.
- Personal information provided by you (such as name or e-mail) will not be disclosed to anyone unless you indicate that Cerner may do so, or as described in this Privacy Policy.
- Only statistical information about *Cerner Direct* users as a group (such as usage habits or demographics) may be shared with any affiliate, subsidiary, or partner of Cerner, unless an appropriate confidentiality agreement is in place.

How Information is Collected and Used

Cerner Direct collects certain information from you in three ways: (i) from *Cerner Direct* web server logs, (ii) with cookies and web analytics tools, and (iii) directly from you.

(a) IP Addresses (Server Log Information). An IP address is a number automatically assigned to your computer whenever you access the Internet. All computer identification on the Internet is conducted with IP addresses, which allow computers and servers to recognize and communicate with each other. *Cerner Direct* collects IP addresses in order to conduct system administration, report Aggregate Information (as defined below) to affiliates, subsidiaries, sponsors, or partners, and to conduct site analysis. *Cerner Direct* will also use IP addresses to identify any users who refuse to comply with the Terms of Use agreement, and to identify users who threaten *Cerner Direct's* service, web site, users, clients or others.

(b) Cookies. *Cerner Direct* places a text file called a "cookie" in the browser files of your computer. Cookies are pieces of information that a web site transfers to an individual's hard disk for record keeping purposes. *Cerner Direct* uses cookies to identify your on-line session, secure your information, and improve the performance of *Cerner Direct*. These cookies do not contain personal information. You may disable cookies in your browser but doing so will restrict your access to only public pages and you will no longer be able to access *Cerner Direct*.

(c) Web Analytics. Cerner may use Google Analytics to understand CernerDirect.com's site usage. Site usage information is used to help design, develop, and support CernerDirect.com. To the extent Cerner uses Google Analytics, Google receives and stores CernerDirect.com's contributed site usage information (such as pages accessed), but it does not receive any individually identifiable or sensitive information as a part of this process. If you do not want data collected by Google Analytics, you can use the Google Analytics Opt-out Browser Add-on available on Google's website.

(d) Registration (User-Supplied Information). *Cerner Direct* registration systems may require you to give Cerner contact information (such as their name and e-mail address) and demographic information (such as a ZIP code, organization and/or role). Your contact information is used to contact you when necessary.

(e) Services (User-Supplied Information). Cerner may use your account and e-mail address to communicate with you about its services. If you sign up for a new service, Cerner may collect personal information such as contact information (e.g. name, address, telephone number and alternate e-mail address), demographic information (e.g. zip code, organization and/or role), billing information (e.g. credit or debit card numbers), or sensitive information (e.g. healthcare information).

How Information is Shared and Disclosed

Cerner does not rent, sell or share personal information about you with other people or nonaffiliated companies, except when Cerner has your permission, or under the following circumstances:

(a) Disclosures to Third Parties Assisting In Our Operations. Cerner may provide your personal information to affiliates, subsidiaries and trusted partners who work on behalf of or with Cerner under confidentiality agreements. These companies may use your personal information to assist Cerner in its operations. However, these companies do not have any independent right to share this information.

(b) Aggregate Information. Cerner may provide information about you that does not allow you to be identified or contacted ("Aggregate Information") to third parties, such as usage information and trends. When Aggregate Information is provided, we pool it from many individual records and strip it of any data that could be used to identify you before it is used.

(c) Disclosures Under Special Circumstances. Cerner may provide information about you to respond to subpoenas, court orders or legal process, or to establish or exercise our legal rights or defend against legal claims. Cerner believes it is necessary to share information in order to investigate, prevent or take legal action regarding illegal activities, suspected fraud, situations involving potential threats to the physical safety of any person, violations of Cerner's Terms of Use, or as otherwise required by law.

(d) Disclosures to Your System Administrator. Your system administrator is the individual or entity who assigned your *Cerner Direct* account to you, such as your employer, a health information exchange or an accountable care organization. Cerner may provide your system administrator with information related to your use of your *Cerner Direct* account, such as usage reports and your compliance with the Terms of Use. Your system administrator may also own your *Cerner Direct* account, in which case they may be able to access the emails within your account.

Information Security

Cerner understands that storing personally identifiable data in a secure manner is essential. *Cerner Direct* data is stored using industry-standard physical, technical and administrative safeguards to secure data against foreseeable risks, such as unauthorized use, access, disclosure, destruction or modification. Cerner's data security practices are consistent with the standards of the Health Insurance Portability and Accountability Act ("HIPAA") security regulations. We regularly review our physical and electronic security measures to manage and enhance our capabilities.

Your Ability to Edit and Delete Your Information

You can edit or delete your personal information that is maintained by Cerner at any time by submitting a request to your *Cerner Direct* system administrator.

Questions

We regularly review our compliance with this Privacy Policy. If you have any questions or suggestions about how we treat personal information, please contact us at:

Cerner Corporation
2800 Rockcreek Parkway
Kansas City, Missouri 64117 U.S.A.
Attention: Chief Legal Officer

Notification of Changes to this Privacy Policy

This Privacy Policy may be revised from time to time as we add new features and services, as laws change, and as industry privacy and security practices evolve. However, Cerner will take reasonable steps to notify you of material changes it makes to the Privacy Policy. We display an effective date on the policy below so that it will be easier for you to know when there has been a change. You are responsible for regularly reviewing this Privacy Policy. Your continued use of *Cerner Direct* constitutes your acceptance of the revised terms. Small changes or changes that do not significantly affect individual privacy interests may be made at any time and without prior notice.

Last Modified: June 28, 2013

PRIVACY POLICY TERMS OF USE CONTACT US