DigiCert

Certification Policy/

Certification Practices Statement for

DirectTrust

DigiCert, Inc.
Version 1.1
8 February 2023
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 7
1.1 OVERVIEW 7
1.2 DOCUMENT NAME AND IDENTIFICATION 7
1.3. PKI PARTICIPANTS 8
1.3.1. DigiCert Policy Management Authority and Certification Authorities 8
1.3.2 Registration Authorities and Other Delegated Third Parties 8
1.3.2.1 Trusted Agents 9
1.3.3. Subscribers 9
1.3.3.1 Custodian 9
1.3.3.2 Health Information Service Provider (HISPs) 9
1.3.3.3 Sponsors 10
1.3.4. Relying Parties 10
1.3.5. Other Participants 10
1.3.5.1 Affiliates 10
1.3.5.2 Affiliated Organizations 10
1.4. CERTIFICATE USAGE 10
1.4.1. Appropriate Certificate Uses 10
1.4.2. Prohibited Certificate Uses 11
1.5. POLICY ADMINISTRATION 11
1.5.1. Organization Administering the Document 11
1.5.2. Contact Person 11
1.5.3. Person Determining CP/CPS Suitability for the Policy 11
1.5.4. CP/CPS Approval Procedures 11
1.6. DEFINITIONS AND ACRONYMS 12
1.6.1. Definitions 12
1.6.2. Acronyms 12
1.6.3. References 13
2. PUBLICATION AND REPOSITORY RESPONSIBILITIES 14
2.1. REPOSITORIES 14
2.2. PUBLICATION OF CERTIFICATION INFORMATION 14
2.3. TIME OR FREQUENCY OF PUBLICATION 14
2.4. ACCESS CONTROLS ON REPOSITORIES 14
3. IDENTIFICATION AND AUTHENTICATION 15
3.1. NAMING 15
3.1.1. Types of Names 15
3.1.2. Need for Names to be Meaningful 15
3.1.3. Anonymity or Pseudonymity of Subscribers 15
3.1.4. Rules for Interpreting Various Name Forms 15
3.1.5. Uniqueness of Names 15
3.1.6. Recognition, Authentication, and Role of Trademarks 15
3.2. INITIAL IDENTITY VALIDATION 16
3.2.1. Method to Prove Possession of Private Key 16

3.2.2. Authentication of Organization Identity *16*
3.2.2.1 Authentication of DirectTrust CE Certificates 17
3.2.2.2 Authentication of DirectTrust BA Certificates 17
3.2.2.3 Authentication of DirectTrust HE Certificates 17
3.2.2.4 Authentication of DirectTrust Non-Declared Certificates 17
3.2.3. Authentication of Individual Identity *18*
3.2.3.1. Authentication of Human Subscribers 18
3.2.3.2. Authentication of Human Subscribers for Role-based Certificates 26
3.2.3.3. Authentication of Human Subscribers for Group Certificates 26
3.2.3.4 Verification Authentication of Devices 27
3.2.3.5 Verification Authentication of Human Subscribers for Content Commitment Certificates 27
3.2.3.6 Verification of NPI Number 27
3.2.4. Non-verified Subscriber Information *28*
3.2.5 Validation of Authority *28*
3.2.6 Criteria for Interoperation *28*
3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS 28
3.3.1. Identification and Authentication for Routine Re-key *28*
3.3.2 Identification and Authentication for Re-Key after Revocation *28*
3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST 28
4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS 29
4.1. CERTIFICATE APPLICATION 29
4.1.1. Who Can Submit a Certificate Application *29*
4.1.2. Enrollment Process and Responsibilities *29*
4.2. CERTIFICATE APPLICATION PROCESSING 29
4.2.1. Performing Identification and Authentication Functions *29*
4.2.2. Approval or Rejection of Certificate Applications *29*
4.2.3. Time to Process Certificate Applications *30*
4.3. CERTIFICATE ISSUANCE 30
4.3.1. CA Actions during Certificate Issuance *30*
4.3.2. Notification to Subscriber by the CA of Issuance of Certificate *30*
4.4. CERTIFICATE ACCEPTANCE 30
4.4.1. Conduct Constituting Certificate Acceptance *30*
4.4.2. Publication of the Certificate by the CA *30*
4.4.3. Notification of Certificate Issuance by the CA to Other Entities *30*
4.5. KEY PAIR AND CERTIFICATE USAGE 30
4.5.1. Subscriber Private Key and Certificate Usage *30*
4.5.2. Relying Party Public Key and Certificate Usage *31*
4.6. CERTIFICATE RENEWAL 31
4.6.1. Circumstance for Certificate Renewal *31*
4.6.2. Who May Request Renewal *31*
4.6.3. Processing Certificate Renewal Requests *31*
4.6.4. Notification of New Certificate Issuance to Subscriber *31*
4.6.5. Conduct Constituting Acceptance of a Renewal Certificate *32*
4.6.6. Publication of the Renewal Certificate by the CA *32*

4.6.7. Notification of Certificate Issuance by the CA to Other Entities *32*
4.7. CERTIFICATE RE-KEY 32
4.7.1. Circumstance for Certificate Re-key *32*
4.7.2. Who May Request Certificate Re-key *32*
4.7.3. Processing Certificate Re-key Requests *32*
4.7.4. Notification of Certificate Re-key to Subscriber *32*
4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate *33*
4.7.6. Publication of the Issued Certificate by the CA *33*
4.7.7. Notification of Certificate Issuance by the CA to Other Entities *33*
4.8 CERTIFICATE MODIFICATION 33
4.8.1 Circumstances for Certificate Modification *33*
4.8.2 Who May Request Certificate Modification *33*
4.8.3 Processing Certificate Modification Requests *33*
4.8.4 Notification of Certificate Modification to Subscriber *33*
4.8.5 Conduct Constituting Acceptance of a Modified Certificate *34*
4.8.6 Publication of the Modified Certificate by the CA *34*
4.8.7 Notification of Certificate Modification by the CA to Other Entities *34*
4.9 CERTIFICATE REVOCATION AND SUSPENSION 34
4.9.1 Circumstances for Revocation *34*
4.9.2 Who Can Request Revocation *34*
4.9.3 Procedure for Revocation Request *34*
4.9.4 Revocation Request Grace Period *35*
4.9.5 Time within which CA Must Process the Revocation Request *35*
4.9.6 Revocation Checking Requirement for Relying Parties *35*
4.9.7 CRL Issuance Frequency *35*
4.9.8 Maximum Latency for CRLs *35*
4.9.9 On-line Revocation/Status Checking Availability *35*
4.9.10 On-line Revocation Checking Requirements *36*
4.9.11 Other Forms of Revocation Advertisements Available *36*
4.9.12 Special Requirements Related to Key Compromise *36*
4.9.13 Circumstances for Suspension *36*
4.9.14 Who Can Request Suspension *36*
4.9.15 Procedure for Suspension Request *36*
4.9.16 Limits on Suspension Period *36*
4.10 CERTIFICATE STATUS SERVICES 36
4.10.1 Operational Characteristics *36*
4.10.2 Service Availability *36*
4.10.3 Optional Features *36*
4.11 END OF SUBSCRIPTION 36
4.12 KEY ESCROW AND RECOVERY 37
4.12.1 Key Escrow and Recovery Policy Practices *37*
4.12.2 Session Key Encapsulation and Recovery Policy and Practices *37*
5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS 38
5.1 PHYSICAL CONTROLS 38

5.1.1 Site Location and Construction *38*
5.1.2 Physical Access *38*
5.1.3 Power and Air Conditioning *39*
5.1.4 Water Exposures *39*
5.1.5 Fire Prevention and Protection *39*
5.1.6 Media Storage *39*
5.1.7 Waste Disposal *39*
5.2 PROCEDURAL CONTROLS 39
5.2.1 Trusted Roles *39*
5.2.1.1 Administrators 40
5.2.1.2 Officers – Validation and Vetting Personnel 40
5.2.1.3 Internal Auditors 40
5.2.1.4 Operator 41
5.2.2 Number of Persons Required per Task *41*
5.2.3 Identification and Authentication for each Role *41*
5.2.4 Roles Requiring Separation of Duties *41*
5.3 PERSONNEL CONTROLS 41
5.3.1 Qualifications, Experience, and Clearance Requirements *41*
5.3.2 Background Check Procedures *42*
5.3.3 Training Requirements *42*
5.3.4 Retraining Frequency and Requirements *42*
5.3.5 Job Rotation Frequency and Sequence *42*
5.3.6 Sanctions for Unauthorized Actions *42*
5.3.7 Independent Contractor Requirements *43*
5.3.8 Documentation Supplied to Personnel *43*
5.4 AUDIT LOGGING PROCEDURES 43
5.4.1 Types of Events Recorded *43*
5.4.2 Frequency of Processing Log *46*
5.4.3 Retention Period for Audit Log *46*
5.4.4 Protection of Audit Log *46*
5.4.5 Audit Log Backup Procedures *46*
5.4.6 Audit Collection System *46*
5.4.7 Notification to Event-causing Subject *46*
5.4.8 Vulnerability Assessments *46*
5.5 RECORDS ARCHIVAL 47
5.5.1 Types of Records Archived *47*
5.5.2 Retention Period for Archive *47*
5.5.3 Protection of Archive *48*
5.5.4 Archive Backup Procedures *48*
5.5.5 Requirements for Time-stamping of Records *48*
5.5.6 Archive Collection System (internal or external) *48*
5.5.7 Procedures to Obtain and Verify Archive Information *48*
5.6 KEY CHANGEOVER 48
5.7 COMPROMISE AND DISASTER RECOVERY 48

5.7.1 Incident and Compromise Handling Procedures *48*
5.7.2 Computing Resources, Software, and/or Data Are Corrupted *49*
5.7.3 Entity Private Key Compromise Procedures *49*
5.7.4 Business Continuity Capabilities after a Disaster *49*
5.8 CA OR RA TERMINATION 49
6 TECHNICAL SECURITY CONTROLS 50
6.1 KEY PAIR GENERATION AND INSTALLATION 50
6.1.1 Key Pair Generation *50*
6.1.1.2 CA Key Pair Generation 50
6.1.1.3 Subscriber Key Pair Generation 50
6.1.2 Private Key Delivery to Subscriber *50*
6.1.3 Public Key Delivery to Certificate Issuer *50*
6.1.4 CA Public Key Delivery to Relying Parties *51*
6.1.5 Key Sizes *51*
6.1.6 Public Key Parameters Generation and Quality Checking *51*
6.1.7 Key Usage Purposes (as per X.509 v3 key usage field) *51*
6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 52
6.2.1 Cryptographic Module Standards and Controls *52*
6.2.2 Private Key (n out of m) Multi-person Control *52*
6.2.3 Private Key Escrow *52*
6.2.4 Private Key Backup *52*
6.2.5 Private Key Archival *53*
6.2.6 Private Key Transfer into or from a Cryptographic Module *53*
6.2.7 Private Key Storage on Cryptographic Module *53*
6.2.8 Method of Activating Private Keys *53*
6.2.9 Method of Deactivating Private Keys *53*
6.2.10 Method of Destroying Private Keys *54*
6.2.11 Cryptographic Module Rating *54*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 54
6.3.1 Public Key Archival *54*
6.3.2 Certificate Operational Periods and Key Pair Usage Periods *54*
6.4 ACTIVATION DATA 54
6.4.1 Activation Data Generation and Installation *54*
6.4.2 Activation Data Protection *55*
6.4.3 Other Aspects of Activation Data *55*
6.4.3.1 Activation of Private Key for Content Commitment 55
6.4.3.2 Authentication for Private Key Activation 55
6.5 COMPUTER SECURITY CONTROLS 56
6.5.1 Specific Computer Security Technical Requirements *56*
6.5.2 Computer Security Rating *57*
6.6 LIFE CYCLE TECHNICAL CONTROLS 57
6.6.1 System Development Controls *57*
6.6.2 Security Management Controls *57*
6.6.3 Life Cycle Security Controls *57*

6.7 NETWORK SECURITY CONTROLS 57
6.8 TIME-STAMPING 58
7 CERTIFICATE, CRL, AND OCSP PROFILES 59
7.1 CERTIFICATE PROFILE 59
7.1.1 Version Number(s) *59*
7.1.2 Certificate Extensions *59*
7.1.3 Algorithm Object Identifiers *59*
7.1.4 Name Forms *59*
7.1.5 Name Constraints *59*
7.1.6 Certificate Policy Object Identifier *59*
7.1.7 Usage of Policy Constraints Extension *60*
7.1.8 Policy Qualifiers Syntax and Semantics *60*
7.1.9 Processing Semantics for the Critical Certificate Policies Extension *60*
7.2 CRL PROFILE 60
7.2.1 Version number(s) *60*
7.2.2 CRL and CRL Entry Extensions *60*
7.3 OCSP PROFILE 61
7.3.1 Version Number(s) *61*
7.3.2 OCSP Extensions *61*
8 COMPLIANCE AUDIT AND OTHER ASSESSMENT 62
8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT 62
8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR 62
8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY 62
8.4 TOPICS COVERED BY ASSESSMENT 62
8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY 62
8.6 COMMUNICATION OF RESULTS 62
9 OTHER BUSINESS AND LEGAL MATTERS 63
9.1 FEES 63
9.1.1 Certificate Issuance or Renewal Fees *63*
9.1.2 Certificate Access Fees *63*
9.1.3 Revocation or Status Information Access Fees *63*
9.1.4 Fees for Other Services *63*
9.1.5 Refund Policy *63*
9.2 FINANCIAL RESPONSIBILITY 63
9.2.1 Insurance Coverage *63*
9.2.2 Other Assets *63*
9.2.3 Insurance or Warranty Coverage for End-Entities *63*
9.3 CONFIDENTIALITY OF BUSINESS INFORMATION 63
9.3.1 Scope of Confidential Information *63*
9.3.2 Information Not Within the Scope of Confidential Information *64*
9.3.3 Responsibility to Protect Confidential Information *64*
9.4 PRIVACY OF PERSONAL INFORMATION 64
9.4.1 Privacy Plan *64*

9.4.2 Information Treated as Private *64*
9.4.3 Information Not Deemed Private *64*
9.4.4 Responsibility to Protect Private Information *64*
9.4.5 Notice and Consent to Use Private Information *64*
9.4.6 Disclosure Pursuant to Judicial or Administrative Process *65*
9.4.7 Other Information Disclosure Circumstances *65*
9.5 INTELLECTUAL PROPERTY RIGHTS 65
9.6 REPRESENTATIONS AND WARRANTIES 65
9.6.1 CA Representations and Warranties *65*
9.6.2 RA Representations and Warranties *66*
9.6.3 Subscriber Representations and Warranties *66*
9.6.4 Relying Party Representations and Warranties *66*
9.6.5 Representations and Warranties of Other Participants *67*
9.7 DISCLAIMERS OF WARRANTIES 67
9.8 LIMITATIONS OF LIABILITY 67
9.9 INDEMNITIES 68
9.9.1 Indemnification by DigiCert *68*
9.9.2 Indemnification by Subscribers *68*
9.9.3 Indemnification by Relying Parties *68*
9.10 TERM AND TERMINATION 69
9.10.1. Term *69*
9.10.2. Termination *69*
9.10.3. Effect of Termination and Survival *69*
9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS 69
9.12 AMENDMENTS 69
9.12.1 Procedure for Amendment *69*
9.12.2 Notification Mechanism and Period *69*
9.12.3 Circumstances under which OID Must Be Changed *70*
9.13 DISPUTE RESOLUTION PROVISIONS 70
9.14 GOVERNING LAW 70
9.15 COMPLIANCE WITH APPLICABLE LAW 70
9.16 MISCELLANEOUS PROVISIONS 70
9.16.1 Entire Agreement *70*
9.16.2 Assignment *70*
9.16.3 Severability *70*
9.16.4 Enforcement (attorneys' fees and waiver of rights) *71*
9.16.5 Force Majeure *71*
9.17 OTHER PROVISIONS 71

1. INTRODUCTION

1.1 OVERVIEW

This document is the DigiCert, Inc. ("DigiCert") Certificate Policy/Certification Practices Statement (CP/CPS) for DirectTrust Services that outlines, in RFC 3647 format, the principles and practices related to DigiCert's certification of non-cross-certified and non-publicly trusted X.509 digital certificates. This document defines the creation and life-cycle management of X.509 version 3 Public Key Certificates for use in applications primarily supporting electronic health information exchange, including Direct exchange.

This CP/CPS is only one of several documents that control DigiCert's certification services for DirectTrust. Other important documents include both private and public documents, such as DigiCert's agreements with its customers, the DirectTrust CP, relying party agreements, Registration Authority Agreements, any applicable Registration Authority Practices Statement (RPS), 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.

Digital Certificates contain at minimum, three registered Certificate policy object identifiers (OIDs), which may be used by a Relying Party to decide whether a Certificate is trusted for a particular purpose. An OID specifying the version of the DirectTrust CP, an OID corresponding to an identity proofing Level of Assurance (LoA), and an OID corresponding to a healthcare category are available to Relying Parties. DigiCert asserts the appropriate OIDs in the certificatePolicies extension of Certificates. DigiCert may assert a mapping between the DirectTrust CP and this CP/CPS in the policyMappings extension of its CA Certificate.

Compliance to an Active CP Version is a requirement for accreditation under the DirectTrust Accreditation Program as described in the DirectTrust CP Section 1.5.3, and DigiCert is audited regarding implementation of practices in compliance with an Active CP Version in conjunction with proper use of the DirectTrust policy OIDs. DirectTrust publishes bundles of trust anchors for the purpose of assisting Relying Parties in verifying the accredited status of Custodians (e.g. HISPs), CAs, and RAs, available at https://www.directtrust.org.

1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the DigiCert Certificate Policy/Certification Practices Statement for DirectTrust services and has been approved for publication by the DigiCert Policy Authority (DCPA) as of the date indicated on the cover page.

Date	Changes	Version
May 6, 2021	Initial draft	1.0
February 8, 2023	Update OID references	1.1

The DirectTrust CP defines multiple levels of assurance each assigned a unique object identifier (OID). The DirectTrust set of policy OIDs are registered under an arc of its assigned organizational

identifier as registered in the ISO/ITU OID Registry. The applicable DirectTrust OIDs pertaining to this CPS and the trust community are created under a DirectTrust arc defined as follows: [iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)]

DigiCert asserts only the OIDs listed below when issuing under the DirectTrust arc. Policy OIDs asserting additional compliance with other CPs, i.e. under a different policy arc may be present.

This document adheres to version 2.0 of the DirectTrust Community X.509 Certificate Policy which is referenced by the Certificate Policy Version OID 1.3.6.1.4.1.41179.0.2.0.

OID Reference		OID
DirectTrust CP	id-DirectTrust policies.(2.0)	1.3.6.1.4.1.41179.0.2.0
DigiCert NIST LoA3 OID		2.16.840.1.114412.4.3.3
DirectTrust LoA3 OID	id-DirectTrust-LoAs.(3)	1.3.6.1.4.1.41179.1.3
HIPAA category OID: (only one of these is asserted in each certificate)		
DirectTrust CE (HIPAA Covered Entity)	d-DirectTrust- Cat.(1)	1.3.6.1.4.1.41179.2.1
DirectTrust BA (HIPAA Business Associate)	id-DirectTrust- Cat.(2)	1.3.6.1.4.1.41179.2.2
DirectTrust HE (other HIPAA Healthcare Entity)	id-DirectTrust- Cat.(3)	1.3.6.1.4.1.41179.2.3
DirectTrust Device	id-DirectTrust-Dev (1)	1.3.6.1.4.1.41179.3.1
DirectTrust Patient	id-DirectTrust- Cat.(4)	1.3.6.1.4.1.41179.2.4

This CPS applies to any entity asserting one or more of the DirectTrust OIDs identified above by DigiCert. All other OIDs mentioned herein belong to their respective owners. Subsequent revisions to this CPS might contain additional OID assignments than those identified above.

1.3. PKI PARTICIPANTS

1.3.1. DigiCert Policy Management Authority and Certification Authorities

A Certification Authority (CA) is an entity that issues Public Key X.509 Certificates and, through such issuance, attests to the binding between an identity and cryptographic Key Pair to a Subscriber. For ease of reference herein, all CAs issuing Certificates in compliance with the DirectTrust CP and this CP/CPS are hereafter referred to as "Issuer CAs".

DigiCert Root Certificate Authorities and Intermediate CAs under the control of DigiCert 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/CPS as well as overseeing the review and conformance of CA practices with the DirectTrust CP with their own respective Policy Management Authorities and legal agreements.

1.3.2 Registration Authorities and Other Delegated Third Parties

Registration Authorities (RA) are organizations responsible for collecting and proofing a

Subscriber's identity and any other information provided by Subscriber for inclusion in a Certificate. All practices and requirements in the DirectTrust CP and this CP/CPS apply to all RAs operating under DigiCert for the DirectTrust program. If DigiCert relies upon an RA for the DirectTrust program, DigiCert will monitor the RA's compliance with the DirectTrust CP and this CP/CPS, and if applicable, any Registration Practices Statement (RPS) under which the RA operates. If RAs are used, DigiCert will only rely on RAs that are accredited as RAs by DirectTrust or DirectTrust-EHNAC to operate in compliance with the DirectTrust CP and this CP/CPS and are approved by the DirectTrust Policy Committee (DTPC).

1.3.2.1 Trusted Agents

Trusted Agents are individuals who act on behalf of DigiCert or an approved RA to collect and/or verify information regarding Subscribers and, where applicable, to provide support regarding those activities to the Subscribers. Trusted Agents are Individuals who, while not an employee of DigiCert or the approved RA, have a direct contractual relationship with DigiCert or the approved RA, either as: a) an Individual; or b) an employee of an Organization that has a direct contractual relationship with DigiCert or the approved RA that involves performance of collection and/or confirmation of information regarding Subscribers.

DigiCert or the approved RA may provide the Trusted Agent with material to facilitate the activities being performed by the Trusted Agent on behalf of DigiCert or the approved RA, including, but not limited to software products, dedicated web pages, electronic or paper forms, instruction manuals and training sessions.

All activities of the Trusted Agent are performed in accordance with the DirectTrust CP, this CP/CPS, and any applicable RA RPS.

1.3.3. Subscribers

Subscribers use DigiCert's services and PKI to support transactions and communications. A Subscriber is an individual, organization or device to whom or to which a Certificate is issued. Subscribers are named in the Certificate Subject and hold, either directly or through its designated Custodian (e.g. HISP or other authorized third party), a Private Key that corresponds to the Public Key listed in the Certificate. A Subscriber, as used herein, refers to both the Subject of the certificate and the entity that contracted with DigiCert for the certificate's issuance.

1.3.3.1 Custodian

A Custodian holds and manages the Private Keys associated with a Subscriber's Certificate. A Custodian is responsible for assuring that all requirements for activation of the Private Key are met prior to any activation of the Private Key. A Custodian acts as a Keystore Operator.

1.3.3.2 Health Information Service Provider (HISPs)

A Health Information Service Provider (HISP) is an entity that processes Direct-

compliant messages to and from Direct Addresses, each of which is bound to a Direct-compliant Certificate. A HISP acts in the capacity of Custodian for the Subscriber for the purposes of Direct messaging.

1.3.3.3 Sponsors

A Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel and non-human system components named as Public Key Certificate Subjects. The Sponsor works with DigiCert and an approved RA to register the above elements in accordance with Section 3.2.2 and 3.2.3 and are responsible for meeting the obligations of Subscribers as defined throughout this document.

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 will review a Subscriber's Certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the Certificate by checking the appropriate certificate status information (CRL or OCSP).

1.3.5. Other Participants

1.3.5.1 Affiliates

An Affiliate is an individual or organization legally distinct from the Subscriber who is permitted by the Subscriber to use the Subscriber's Certificate, provided that the Affiliate is performing its work, duties or activities on behalf of the Subscriber when using that Certificate.

1.3.5.2 Affiliated Organizations

Subscriber Certificates may be issued in conjunction with an organization that has a relationship with the Subscriber; this is termed organizational affiliation. The organizational affiliation will be indicated in the Certificate. Affiliated Organizations are responsible for verifying the affiliation at the time of Certificate application and requesting revocation of the certificate if the affiliation is no longer valid.

1.4. CERTIFICATE USAGE

A digital certificate (or certificate) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction.

1.4.1. Appropriate Certificate Uses

The primary anticipated use for DirectTrust Certificates is for the secure exchange of electronic information for healthcare purposes. Relying Parties are expected to evaluate the application environment and associated risks before deciding whether to accept a Certificate

issued under this CP/CPS for any particular purpose.

An Affiliate that is a healthcare provider or healthcare organization can only use the Certificate of a Subscriber if that Affiliate provides care on behalf of the Subscriber and the Subscriber is a HIPAA Covered Entity. A Covered Entity can only be an Affiliate of another Covered Entity and cannot be an Affiliate of a Business Associate, except when the Covered Entity is providing services to or on behalf of the Business Associate. For example, an HIE (Business Associate) does not allow use of its own Certificate by a member healthcare provider or member healthcare organization (Covered Entity).

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. Certificates issued under this CP/CPS cannot be used where prohibited by law.

1.5. POLICY ADMINISTRATION

1.5.1. Organization Administering the Document

This CP/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

1.5.2. Contact Person

Attn: Legal Counsel DigiCert Policy Authority
Suite 500
2801 N. Thanksgiving Way
Lehi, UT 84043 USA

1.5.3. Person Determining CP/CPS Suitability for the Policy

The DCPA determines the suitability and applicability of this CP/CPS based on the contract with the customer for which the PKI is operated and any relevant audits. The DCPA is responsible for the PKI's compliance of this CP/CPS with the DirectTrust CP.

1.5.4. CP/CPS Approval Procedures

The DCPA approves the CP/CPS and any amendments. Amendments are made after the DCPA has reviewed the amendments' consistency with relevant contracts and the

DirectTrust CP. The DCPA determines whether an amendment to this CP/CPS is consistent with a contract, requires notice, or requires an OID change. The DirectTrust Board of Directors managing the DirectTrust CP will determine if this CP/CPS conforms to by contract, approve this CP/CPS for each CA that issues certificates under that respective CP.

1.6. DEFINITIONS AND ACRONYMS

1.6.1. Definitions

"Applicant" means an entity applying for a certificate.

"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.

"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.

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

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

"Superior Entity" An entity above a certain entity within the PKI.

1.6.2. Acronyms

CA	Certificate Authority or Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DCPA	DigiCert Policy Authority

FIPS	(US Government) Federal Information Processing Standard
HSM	Hardware Security Module
IdM	Identity Management System
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
PMA	Policy Management Authority
RA	Registration Authority
RPS	Registration Authority Practices Statement
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

1.6.3. References

No stipulation.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1. REPOSITORIES

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 via URIs included in the certificates themselves in the X.509v3 extension
2. By email to support@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

DigiCert and end entity Certificates for DirectTrust only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties. DigiCert publishes its CA Certificate and any other intermediate or trust anchor Certificates necessary to validate the Issuer CA for DirectTrust. For all other information, DigiCert protects information not intended for public dissemination through the request process listed above. This CP/CPS will be made available in the DigiCert Legal Repository located here: https://www.digicert.com/legal-repository

2.3. TIME OR FREQUENCY OF PUBLICATION

CRLs for end-user certificates are issued before the nextUpdate period listed in the CRL endpoints in the certificate. CRLs for CA Certificates are issued in accordance with the agreements made with DirectTrust. New or modified versions of this CP/CPS, Subscriber Agreements, or Relying Party Warranties are typically published within seven days after their approval.

2.4. ACCESS CONTROLS ON REPOSITORIES

DigiCert and authorized RAs protect repository information not intended for public dissemination or modification. Read-only access to the repository is unrestricted. Logical and physical controls internal to DigiCert prevent unauthorized write access to repositories.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

Certificates are issued with a subject Distinguished Name (DN) that complies with ITU X.500 standards. Some certificates may have a null subject DN if it includes at least one alternative name form that is marked critical.

Address-Bound Certificates contain a full Direct Address in the form of an rfc822Name in the Subject Alternative Name (also referred to as subjectAltName) extension of the Certificate.

Domain-Bound Certificates contain a Health Domain Name in the form of a dNSName in the subject common name and Subject Alternative Name extensions of the Certificate.

3.1.2. Need for Names to be Meaningful

DigiCert uses distinguished names to identify the subject (i.e. person, organization, device, or object) or issuer of the certificate.

Subscriber certificates contain meaningful names with commonly understood semantics permitting the determination of the identity of the organization that is the Subject of the certificate by DigiCert and by designated RAs. RAs will describe this process in their associated RPS.

3.1.3. Anonymity or Pseudonymity of Subscribers

DigiCert does not issue anonymous Certificates for DirectTrust. Pseudonymous Certificates may be issued as long as 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

DigiCert enforces name uniqueness of the Certificate subject DN within the CA's X.500 namespace. RAs are required to enforce name uniqueness in communities where they participate.

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. Unless otherwise specifically stated in an agreement with a customer, 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. Participating RAs must specify the validation methods used to verify identity information in their applicable RPS.

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.

Certificates generated by DigiCert require proof that the Subscriber possesses the private key. In the case where the Subscriber generates its own Private Key, then the Subscriber digitally signs a known piece of data with the Private Key and send it to DigiCert or the approved RA. DigiCert or the RA will verify the signature and the known piece of data thus proving Private Key possession. Typically, the RA verifies this by verifying the subscriber's digital signature on the PKCS #10 Certificate Signing Request (CSR) with the public key in the CSR. If DigiCert generates the key pair on behalf of the subscriber, proof of possession by the subscriber is not required.

The process of proving possession of the private key for end-entity certificates by RAs will be described in their respective RPS.

3.2.2. Authentication of Organization Identity

Requests for Certificates that assert an organization name in the subject field or Subject Alternative Name extension of the certificate include the organization name, mailing address, and documentation of the legal existence of the organization. For Address-Bound and Domain-Bound Certificates, the requested Health Domain Name or Health Endpoint Name that will appear in the Certificate MUST also be included (see section of the DirectTrust CP and this CP/CPS 3.1.1 for details).

The requesting organization represents to DigiCert and/or an approved RA in a signed statement such as a Certificate application their healthcare category as defined by HIPAA at 45 CFR 160.103. Any organization not providing attestation to one of the above categories is considered a Non-Declared Entity.

An organization acting as a Subscriber or named in a Certificate that asserts organization affiliation, is a legally distinct entity. If a domain name or email address (RFC822 name) is asserted in the Certificate, then the Subscriber will confirm with DigiCert or the RA the right to use it using methods in this section.

For all Certificates asserting an organization name, the DigiCert or the RA verifies the organization and the organization's category in accordance with the following practices to

meet the DirectTrust CP requirements. The organization's category OID will be asserted in all Certificates.

For certificates issued by RAs, the practices that fulfill the requirements will be described in the respective RPS.

3.2.2.1 Authentication of DirectTrust CE Certificates

Applicant represents in a statement such as a signed Certificate application that it is a Covered Entity (CE) as defined by HIPAA at 45 CFR 160.103.

DigiCert or the RA verifies the application includes the signed statement, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization.

3.2.2.2 Authentication of DirectTrust BA Certificates

The Applicant represents in a statement such as a signed Certificate application that it is a Business Associate (BA) as defined by as defined by HIPAA at 45 CFR 160.103.

DigiCert or the RA verifies the application includes the signed statement, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization.

3.2.2.3 Authentication of DirectTrust HE Certificates

The Applicant represents in a statement, such as a signed Certificate application, that it is a Non- HIPAA Healthcare Entity (HE), defined as an entity that is not covered by HIPAA and handles Protected Health Information in accordance with HIPAA Privacy and Security Rules as required for Covered Entities.

DigiCert or the RA verifies the application includes the signed statement, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization.

3.2.2.4 Authentication of DirectTrust Non-Declared Certificates

The applying Entity has not asserted it will protect personal health information with privacy and security protections that are equivalent to those required by HIPAA and is not a Patient. DigiCert or the RA will verify the application, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization.

If a Certificate asserts an organizational affiliation, DigiCert or the RA will obtain documentation from the organization that authorizes the affiliation and an

agreement which obligates the organization to:

- Request modification or revocation of the Certificate if information in the Certificate subject is no longer accurate, and
- Request revocation of unexpired Certificates if organizational affiliation ends.

See also sections 3.2.3.3, 4.9.1 and 9.6.1 of the DirectTrust CP.

3.2.3. Authentication of Individual Identity

3.2.3.1. Authentication of Human Subscribers

DigiCert requires Identity proofing for an individual acting as a:

1. Subscriber;
2. Organizational representative;
3. Information System Security Officer (ISSO); and
4. Sponsor of a Device Certificate.

DigiCert follows the DirectTrust Levels of Assurance that are intended to provide equivalent identity proofing assurance levels to those defined by NIST SP 800-63-2 or NIST SP 800-63-3, further described in the "Guidance for Authentication of Individual Identity", a companion document to this CP. At a minimum, DigiCert or an authorized RA obtains proof of an individual's identity in accordance with one of the following assurance levels:

DirectTrust Level of Assurance	**Identification and Authentication**
DirectTrust LoA 1	DirectTrust requires that the name associated with the Applicant is provided by the Applicant and accepted without verification. DigiCert verifies an individual's or organization's right to use or control an email address to be contained in a Certificate that will have the "Secure Email" EKU by doing one of the following: DigiCert validates the Applicant's right to use or control each domain name that will be listed in the Subject Alternative Name field of a Certificate by using at least one of the following procedures. 1. By verifying domain control over the email domain using one of the following procedures: 1. Email, Fax, SMS, or Postal Mail to the Domain

	Contact by sending a unique Random Value (valid for no more than 30 days from its creation) through email, fax, SMS, or postal mail, to the Domain Contact and receiving confirmation by their use of the Random Value; 2. Constructed Email to Domain Contact establishing the Applicant's control over the FQDN by sending an email created by using 'admin', 'administrator', 'webmaster', 'hostmaster' or 'postmaster' as the local part followed by the ("@") sign, followed by an Authorization Domain name, including a Random Value in the email, and receiving a response using the Random Value. 3. Domain Name Service (DNS) Change by confirming the presence of a Random Value or Request Token in a DNS CNAME, TXT, or CAA record for either an Authorization Domain Name or an Authorization Domain Name prefixed with a label that begins with an underscore character. 4. IP Address - by confirming the Applicant's control over the FQDN through control of an IP address returned from a DNS lookup for A or AAAA records for the FQDN. 5. Confirming that the Applicant is the Domain Contact for the Base Domain Name (provided that the CA or RA is also the Domain Name Registrar or an Affiliate of the Registrar). 6. Confirming the Applicant's control over the FQDN by sending a Random Value via email and then receiving a confirming response utilizing the Random Value. The Random Value will be sent to a DNS CAA Email Contact. The relevant CAA Resource Record Set is found using the search algorithm defined in RFC 6844 Section 4, as amended by Errata 5065. 7. Confirming the Applicant's control over the FQDN by sending a Random Value via email to the DNS TXT Record Email Contact for the Authorization Domain Name for the FQDN and then receiving a confirming response utilizing the Random Value. 8. Confirming the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same Domain Contact

	phone number is listed for each authorized Domain. 9. Confirming the Applicant's control over the FQDN by calling the DNS TXT Record Phone Contact's phone number and obtaining a confirming response to validate the authorized Domain Name. Each phone call can confirm control of multiple authorized Domain Names provided that the same DNS TXT Record Phone Contact phone number is listed for each authorized Domain Name being verified and they provide a confirming response for each authorized Domain Name. 10. Confirming the Applicant's control over the FQDN by calling the DNS CAA Phone Contact's phone number and obtain a confirming response to validate the ADN. Each phone call can confirm control of multiple ADNs provided that the same DNS CAA Phone Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN. 11. Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file (such as a Request Token, Random Value that does not appear in the request used to retrieve the file and receipt of a successful HTTP 2xx status code response from the request). 12. Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in section 8.3 of RFC 8555, performed in accordance with section 8.3 of RFC 8555 as prescribed. 13. Confirming the Applicant's control over a FQDN by validating domain control of the FQDN by negotiating a new application layer protocol using the TLS Application- Layer Protocol Negotiation (ALPN) Extension performed in accordance with RFC 8737. Or: 2. By sending an email message containing a Random Value to the email address to be included in the Certificate and receiving a confirming response through use of the Random Value to indicate that the Applicant and/or Organization owns or controls that same email address.

DirectTrust LoA 2 – In-Person Vetting	The Applicant supplies full legal name, an address of record, and date of birth. For in-person vetting, the Applicant also provides valid government issued photo ID. DigiCert or the approved RA inspects the photo-ID; compares picture to Applicant; and records the ID number, address and date of birth (DoB). DigiCert will issue the credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at the claimed address– or – sends notice to the confirmed physical address associated with the Applicant in the records after issuance.
DirectTrust LoA 2 – Remote Vetting	For remote vetting, the Applicant provides a valid government issued ID identifier and a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID or account. DigiCert or the approved RA inspects both ID and account numbers supplied (e.g. for correct number of digits) and verifies either the ID number OR the account number information provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. (For utility or financial account numbers, confirmation may be performed by verifying knowledge of recent account activity). DigiCert will issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in the records – or – sends notice to an address confirmed in the records check after issuance. Any of the identity proofing methods listed for a higher level

	are also acceptable.
DirectTrust LoA 3 - In-Person Vetting	The Applicant supplies full legal name, an address of record, and date of birth. For in-person vetting, the Applicant also provides a valid government issued photo ID. DigiCert or the approved RA inspects the photo-ID and records the ID number; compares picture to Applicant; and verifies information provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application. DigiCert will issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications at phone number associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at the claimed address– or – sends notice to the confirmed physical address associated with the Applicant in the records after issuance. If the telephone method is used, DigiCert or the RA will record the Applicant's voice or uses alternative means that establish an equivalent level of non-repudiation.
DirectTrust LoA 3 Remote Vetting	For remote vetting, the Applicant provides a valid government issued ID identifier and a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID or account. DigiCert or the approved RA verifies both ID and account numbers provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application. (For utility or financial account numbers, confirmation may be performed by verifying knowledge of recent account activity). DigiCert will issue credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at a physical address

	associated with the Applicant in the records. Any of the identity proofing methods listed for a higher level are also acceptable.
DirectTrust IAL 1	DirectTrust LoA1 and DirectTrust IAL 1 are interchangeable and equivalent and therefore have the same OID. See the first entry in this table for vetting requirements.
DirectTrust IAL2 In-Person Vetting[1]	**Acceptable Evidence:** As evidence of their claimed identity, the Applicant provides: • US Passport, OR • REALID driver's license/REALID ID card, OR • Enhanced driver's license/Enhanced ID card, OR • Other acceptable evidence as described in the "Guidance for Authentication of Individual Identity." **Validation:** Evidence presented by the Applicant is confirmed as genuine by trained RA personnel from DigiCert or an approved RA and/or appropriate technologies including the integrity of any physical and cryptographic security features. All evidence and personal details from the evidence is confirmed as valid by comparison with information held or published by the issuing or authoritative sources and are consistent with the full legal name, address of record and date of birth of the claimed identity. The information printed on the physical evidence listed above is deemed information published by the issuing source. **Verification:** The Applicant's ownership of the claimed identity is confirmed by physical comparison to the photograph or biometrics of the Applicant to the strongest piece of identity evidence provided to support the claimed identity. Additional requirements on the verification of biometrics is provided in the "Guidance for Authentication of Individual Identity". DigiCert will issue credentials to the Applicant in a manner that confirms the address associated with the Applicant in the records. CA issues certificate and delivers it in a secure manner to the appropriate Subscriber.
DirectTrust IAL2	**Acceptable Evidence:**

[1] IAL 2 may be considered a higher level of assurance that meets or exceeds the requirements of IAL 1, LoA 1, LoA 2 and LoA 3.

Remote Vetting (Unsupervised)[2]	As evidence of their claimed identity, the Applicant provides: • US Passport, OR • REALID driver's license / REALID ID card, OR • Enhanced driver's license / Enhanced ID card, OR • Other acceptable evidence as described in the "Guidance for Authentication of Individual Identity." **Validation:** Evidence presented by the Applicant are confirmed as genuine by DigiCert or authorized RA trained RA personnel and/or appropriate technologies including the integrity of any physical and cryptographic security features. All evidence and personal details from the evidence are confirmed as valid by comparison with information held or published by the issuing or authoritative sources and are consistent with the full legal name, address of record and date of birth of the claimed identity. The information printed on the physical evidence listed above is deemed information published by the issuing source. **Verification:** The Applicant's ownership of the claimed identity is confirmed by physical comparison to the photograph or biometrics of the Applicant to the strongest piece of identity evidence provided to support the claimed identity. Additional requirements on the remote verification of biometrics or photograph is provided in the "Guidance for Authentication of Individual Identity." DigiCert or the approved RA sends an enrollment code, with at least six random alphanumeric characters, to a postal address (preferred), mobile telephone (SMS or voice), landline telephone or email that has been validated in records. Depending on the method sent, the enrollment code will remain valid for a maximum duration as follows: • postal address – 10 days • telephone – 10 minutes • email – 24 hours Upon receipt of the valid enrollment code, DigiCert or the RA issues the certificate and delivers it in a secure manner to the appropriate Subscriber and delivers a notification of proofing to a confirmed address of record, different from the

[2] IAL 2 may be considered a higher level of assurance that meets or exceeds the requirements of IAL 1, LoA 1, LoA 2 and LoA 3.

	destination address of record for the enrollment code unless that destination was a postal address.
DirectTrust IAL 3 In-Person Vetting	**Acceptable Evidence:** As evidence of their claimed identity, the Applicant provides evidence aligned with Identity Assurance Level 3 requirements as described in the "Guidance for Authentication of Individual Identity." **Validation:** Evidence presented by the Applicant is confirmed as genuine by DigiCert or authorized RA trained RA personnel and/or appropriate technologies including the integrity of any physical and cryptographic security features. All evidence and personal details from the evidence is confirmed as valid by comparison with information held or published by the issuing or authoritative sources and are consistent with the full legal name, address of record and date of birth of the claimed identity. The information printed on the physical evidence listed above is deemed information published by the issuing source. **Verification:** The Applicant's ownership of the claimed identity is confirmed by physical comparison to the biometrics of the Applicant to the strongest piece of identity evidence provided to support the claimed identity. Additional requirements on the verification of biometrics are provided in the "Guidance for Authentication of Individual Identity". DigiCert issues credentials to the Applicant in a manner that confirms the address associated with the Applicant in the records and a notification of proofing is sent to the confirmed address of record. DigiCert issues the certificate and delivers it in a secure manner to the appropriate Subscriber.
DirectTrust IAL 3 Remote Vetting	Remote Vetting is not permitted per the DirectTrust CP.
DirectTrust Patient	Applicant represents that the Certificate applied for will be used for health information exchange purposes. DigiCert or the RA verifies that the Applicant has made this representation. For Patient Certificates, DigiCert or the RA must proof the

	Patient identity in accordance with any of the above LoA requirements, collect the Subscriber Representation, and asserts in the Certificate the DirectTrust Patient OID and the appropriate LoA OID.

Any government issued ID provided by the Applicant that includes an expiration date must be current and unexpired.

In-Person vetting for LoA 2, LoA 3, LoA4, IAL1, IAL2 and IAL3 may be performed by the RA, Trusted Agent of the RA or an entity certified by a State or Federal Entity as being authorized to confirm identities. A trust relationship between the Trusted Agent and the Applicant which is based on an in-person antecedent may suffice as meeting the In-Person identity vetting requirements for LoA 2, LoA 3 LoA 4, IAL 1, IAL 2 or IAL 3.

3.2.3.2. Authentication of Human Subscribers for Role-based Certificates

Role based Certificates are considered Group Certificates under the DirectTrust CP and this CP/CPS and are verified in accordance with Section 3.2.3.3.

3.2.3.3. Authentication of Human Subscribers for Group Certificates

A Group Certificate is a Certificate where the corresponding Private Key is shared by multiple entities acting in one capacity. A DirectTrust Certificate that is held and managed by the Custodian (e.g. a Health Information Service Provider "HISP" or other authorized third party) on behalf of a Subscriber is an example of a Group Certificate. Identity Proofing of the Subscriber organization and its representative is covered in sections 3.2.2 and 3.2.3.1 in this DirectTrust CP and this CP/CPS.

For Custodian-managed Certificates, DigiCert or the RA will also record the information identified in Section 3.2.3.1 for the ISSO (or equivalent) of the Custodian, before issuing the Certificate. In addition to the authentication of the Subscriber (and their organization when required), the following procedures be performed:

- The Custodian ISSO or equivalent is responsible for ensuring control of the Private Key, including maintaining a list of any Users who have access to or use of the Private Key, and accounting for which User had control of the Private Key at what time.
- The subjectName DN must not imply that the subject is a single individual, e.g. by inclusion of a human name form without also clearly indicating the group nature of its issuance; and
- The Custodian ISSO or equivalent shall maintain a list of those holding the shared Private Key that must be provided to, and retained by, the applicable CA or its designated representative.

Users are identity proofed at a level corresponding to the Level of Assurance

asserted in the Certificate. If the identity proofing component is performed by the Subscriber Organization, then the compliant RA will retain documentation that the Subscriber Organization is bound through a legally binding contract with or an attestation to the RA to identity proof Users in accordance with the requirements corresponding to the LoA of the associated Certificate. This information is made available by the Subscriber Organization to the RA upon request.

3.2.3.4 Verification Authentication of Devices

DigiCert may issue a Certificate for use on or by a Device. In such cases, the Device is required to have a human Sponsor who provides:

- Equipment identification (e.g. , Health Domain Name, DNS name, Device identifier, or Health Endpoint Name associated with Device);
- Equipment Public Keys;
- Equipment authorizations and attributes (if any are to be included in the Certificate); and
- Contact information.

Registration includes identity proofing of the Sponsor as an individual to an assurance level commensurate with the Certificate assurance level being requested for the Device.

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

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

If the Sponsor of a Certificate changes, the new Sponsor reviews the status of each Device to ensure it is still authorized to receive Certificates. These requirements are specified in the Subscriber Agreement signed prior before issuance, requiring that the Certificate details be accurate at all times.

3.2.3.5 Verification Authentication of Human Subscribers for Content Commitment Certificates

Although the Private Key of a Content Commitment certificate may be held and managed by a Custodian on behalf of the Subscriber, this CP requires that procedures be in place such that use and activation of the private key is limited to the Subscriber and not shared with the Custodian. Therefore, a Content Commitment certificate is not considered a Group Certificate.

3.2.3.6 Verification of NPI Number

If the NPI Number is included in a Certificate, it is verified against the NPI Registry

provided by the Centers for Medicare & Medicaid Services (CMS). DigiCert or the RA utilizes the Applicant-provided NPI number to retrieve the Applicant's record from the NPI Registry and confirm that the data elements returned are consistent with the information provided in the application.

3.2.4. Non-verified Subscriber Information

Non-verified Subscriber information is not included in a Certificate by DigiCert or by the RA.

3.2.5 Validation of Authority

See Section 3.2.2.

3.2.6 Criteria for Interoperation

See section 3.2.6 of the DirectTrust CP.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

If a DirectTrust Certificate is revoked, other than during a renewal or update action, the Subscriber must go through the initial identity proofing process described in section 3.2 of this CP/CPS to obtain a new Certificate.

3.3.1. Identification and Authentication for Routine Re-key

If a DirectTrust Certificate is revoked, other than during a renewal or update action, the Subscriber is required to go through the initial identity proofing process described in section 3.2 of this CP/CPS to obtain a new Certificate.

3.3.2 Identification and Authentication for Re-Key after Revocation

If a DirectTrust Certificate is revoked, other than during a renewal or update action, the Subscriber is required go through the initial identity proofing process described in section 3.2 of this CP/CPS to obtain a new Certificate.

3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

DigiCert or an RA authenticates all revocation requests per the CP and relevant legal agreements. DigiCert may authenticate revocation requests by referencing the use of the Private Key corresponding to the certificate's Public Key, regardless of whether the associated Private Key is compromised. If an RA performs validation for a revocation, they will specify the practices to meet the requirements of the contractual agreements, the CP, this CP/CPS, and the associated technical requirement documents in their RPS.

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 per section 1.2 of this CP/CPS may submit certificate requests. Applicants are responsible for any data that the Applicant or an agent of the Applicant supplies to DigiCert or an RA.

4.1.2. Enrollment Process and Responsibilities

A Subscriber is responsible for providing accurate information about himself and his organization during identity proofing. DigiCert or the authorized RA are responsible for ensuring that the identity of each Applicant is proofed in accordance with this CP/CPS prior to the issuance of a Certificate. DigiCert and the approved RA authenticate and protect all communication made during the Certificate application process.

In no particular order, this protected enrollment process may include:

- Submitting a certificate application including the required documentation for the type of DirectTrust Certificate requested,
- Generating a key pair,
- Delivering the public key of the key pair to DigiCert,
- Agreeing to the applicable Subscriber Agreement, and
- Paying any applicable fees.

4.2. CERTIFICATE APPLICATION PROCESSING

DigiCert and the approved RA verify that the information in a CSR is accurate and reflect the information presented by the Subscriber by following the requirements and practices of this section.

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. 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 in accordance with sections 5.4 and 5.5. After verification is complete, DigiCert or the RA evaluates the corpus of information and decides whether or not to issue the certificate. DigiCert considers a source's availability, purpose, and reputation when determining whether a third-party source is reasonably reliable.

4.2.2. Approval or Rejection of Certificate Applications

DigiCert may reject a certificate application if DigiCert believes that issuing the certificate could damage or diminish DigiCert's reputation or business or it does not fulfill the requirements of the associated legal agreements or the DirectTrust CP. RAs may only approve a Certificate Application after verifying the applicant meets all requirements listed

in the DirectTrust CP, this CP/CPS, or any associated guidelines.

4.2.3. Time to Process Certificate Applications

No stipulation.

4.3. CERTIFICATE ISSUANCE

4.3.1. CA Actions during Certificate Issuance

DigiCert or the RA verifies the source of a certificate request before issuance. DigiCert ensures that all Certificate fields and extensions are properly populated. 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

The Subscriber is notified via physical mail, or email or an equivalent means that the Certificate has been issued. Generally, DigiCert delivers certificates by providing the Subscriber a hypertext link to a user id/password-protected location where the subscriber may log in and download the certificate or 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 end-entity certificates by delivering them to the Subscriber and through the methods described in section 2.1.

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

Subscribers or authorized Custodians are 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 as specified by the certificatePolicies, keyUsage and extKeyUsage extensions of the corresponding Certificate.

4.5.2. Relying Party Public Key and Certificate Usage

Certificates comply with the policies provided by DirectTrust. Relying Parties are expected to understand these policies. DigiCert publishes repositories for checking as specified in section 2.1. Relying Parties are expected to review the CRL on a regular basis and reject Certificates found on it and/or respect the Certificate status reflected in an OCSP response.

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.

4.6. CERTIFICATE RENEWAL

Certificate renewal consists of issuing a new Certificate with a new validity period and serial number while retaining all other information in the original Certificate including the Public Key. After Certificate renewal, the old Certificate may or may not be revoked, but cannot be further re-keyed, renewed, or modified.

4.6.1. Circumstance for Certificate Renewal

DigiCert may renew a certificate if:

- The associated Public Key has not reached the end of its validity period,
- The Subscriber and attributes are consistent, and
- 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.

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. 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 in section 3.2 of this CP/CPS or executed via proof of possession of the Private Key through a digital signature. DigiCert or an RA may refuse to renew a certificate if it cannot verify any rechecked information.

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 and in accordance of section 2.1.

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 in accordance with section 2.1.

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

No Stipulation.

4.7. CERTIFICATE RE-KEY

Re-keying a Certificate consists of creating new Certificates with a different Public Key (and serial number) while retaining the remaining contents of the old Certificate that describe the subject. The new Certificate may be assigned a different validity period, key identifiers, specify a different CRL distribution point or OCSP responder location, and/or be signed with a different key. Re-key of a Certificate does not require a change to the subjectName and does not violate the requirement for name uniqueness.

After Certificate re-key, the old Certificate may or may not be revoked, but cannot be further re-keyed, renewed, or modified.

4.7.1. Circumstance for Certificate Re-key

A Certificate is re-keyed when it can no longer be renewed as described in section 4.6.1. A revoked Certificate cannot be re-keyed.

4.7.2. Who May Request Certificate Re-key

DigiCert will only accept re-key requests from the subject of the certificate or the authorized representative of the Subscriber. 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 Re-key Requests

DigiCert or the RA will approve or reject Subscriber Certificate re-keying requests. Identity proofing of the Subscriber is the equivalent to the initial identity proofing or executed via proof of possession of the Private Key through a digital signature.

4.7.4. Notification of Certificate Re-key to Subscriber

See section 4.3.2.

4.7.5. Conduct Constituting Acceptance of a Re-keyed Certificate

See section 4.4.1.

4.7.6. Publication of the Issued Certificate by the CA

See section 4.4.2.

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

See section 4.4.3.

4.8 CERTIFICATE MODIFICATION

Certificate modification consists of creating a new Certificate with subject information (e.g., a name or email address) that differs from the old Certificate. The new Certificate may have the same or different subject Public Key.

After Certificate modification, the old Certificate is not further re-keyed, renewed, or modified. Whether or not the old Certificate is required to be revoked is determined in accordance with section 4.9

4.8.1 Circumstances for Certificate Modification

DigiCert or an RA may modify certificates in the following circumstances:

- For a Subscriber organization name change or other Subscriber characteristic change; or
- To correct subject name attributes or extension settings.

The original certificate may be revoked, but cannot be further re-keyed, renewed, or modified.

4.8.2 Who May Request Certificate Modification

DigiCert or an RA modifies certificates when the Subscriber or their authorized representative or the RA requests modification.

4.8.3 Processing Certificate Modification Requests

Identity proofing for a Certificate modification request is done by DigiCert or an RA using one of the following processes:

- Initial identity proofing process as described in Section 3.2, or
- Identity proofing for re-key as described in Section 3.3, except the old key can be used as the new key.

4.8.4 Notification of Certificate Modification to Subscriber

See section 4.3.2.

4.8.5 Conduct Constituting Acceptance of a Modified Certificate

See section 4.4.1.

4.8.6 Publication of the Modified Certificate by the CA

See section 4.4.2.

4.8.7 Notification of Certificate Modification by the CA to Other Entities

See section 4.4.3.

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. A DirectTrust Certificate will be revoked when the binding between the subject and the subject's Public Key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding include, but are not limited to:

- The identifying information or affiliation components of any names in the Certificate become invalid;
- The Subscriber can be shown to have violated the stipulations of the Subscriber agreement;
- The service agreement between the Subscriber and the Custodian (e.g. HISP) that holds the Private Key ends;
- The Private Key is compromised or is suspected of compromise;
- The Subscriber, Custodian (e.g. HISP) or RA requests Certificate revocation.

DigiCert processes revocation requests in accordance with instructions from the RA and Subscribers. Generally, DigiCert revokes certificates in a reasonable timeframe after receiving an approved revocation request – generally within 24 hours.

If DigiCert or the RA makes the decision to revoke, the associated certificate will be revoked and distributed via OCSP or CRL (as applicable). Revocation information for certificates are included on all new publications of the certificate status information until the certificates expire.

4.9.2 Who Can Request Revocation

The Subscriber, an authorized representative, the RA or DigiCert can request revocation of a Certificate.

4.9.3 Procedure for Revocation Request

Any request for Certificate revocation, other than a request from DigiCert or the Subscriber/Authorized Representative, must identify the Certificate to be revoked by serial

number and explain the reason for revocation. DigiCert or the RA ensures that the Certificate revocation request is not malicious and will verify that the reason for revocation is valid.

For DirectTrust Certificates, DigiCert accepts revocation requests directly from the HISP Administrator. Once confirmed, DigiCert will revoke the Certificate as soon as possible in accordance with section 4.9.6.

If the reason for revocation is valid or the request originates from the Subscriber, DigiCert will revoke the Certificate and place the Certificate's serial number and any other necessary information on its CRL and, if OCSP is supported, have its revoked status reflected in OCSP responses.

4.9.4 Revocation Request Grace Period

There is no grace period for revocation under the DirectTrust CP and program. Subscribers and other participants are required to request the revocation of a Certificate as soon as the need for revocation comes to their attention.

4.9.5 Time within which CA Must Process the Revocation Request

DigiCert begins the investigation of a certificate revocation request promptly after receipt. DigiCert is required by DirectTrust to process all revocation requests within 8 hours of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirement for Relying Parties

Relying Parties must check the status of certificates on which they wish to rely on by checking the certificate status using CRLs or OCSP responses, as applicable.

4.9.7 CRL Issuance Frequency

DigiCert issues fresh CRLs to the repository listed in section 2.2.1 at a maximum interval of 31 days when there are no changes or within 24 hours if there is a change to the CRL. The next Update time for a published CRL is no more than 31 days after the CRL is published.

DigiCert ensures that superseded CRLs are removed from the public repository upon posting of the latest CRL.

4.9.8 Maximum Latency for CRLs

CRLs are posted within four hours after generation. Furthermore, a new CRL is published no later than the time specified in the next Update field of the most recently published CRL.

4.9.9 On-line Revocation/Status Checking Availability

If specified in the certificate, DigiCert provides OCSP response information for issued certificates.

4.9.10 On-line Revocation Checking Requirements

A Relying Party for DigiCert Private PKI Certificates must check the status of a certificate on which they wish to rely on with methods as specified in this section.

4.9.11 Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12 Special Requirements Related to Key Compromise

Revocation information for CA Certificates are published after creation of the appropriate CRL and OCSP information, as applicable. Typically, revocation information for CA Certificates is published within 18 hours.

4.9.13 Circumstances for Suspension

Suspension is not supported.

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 may be available via CRL and OCSP responder. The Repository is available via HTTP or another accessible transfer protocol as specified in section 2.1. 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.

4.10.2 Service Availability

Certificate status services are available on a continuous basis.

4.10.3 Optional Features

OCSP Responders may not be available for all certificate types. For those that are required, they will be configured per the profile requirements of the DirectTrust program.

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. A Subscriber with an unexpired Certificate who is no longer using the Certificate in an approved manner (e.g., for Direct Project secure communications) should have their Certificate revoked.

4.12 KEY ESCROW AND RECOVERY

4.12.1 Key Escrow and Recovery Policy Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 PHYSICAL CONTROLS

DigiCert and RA equipment is protected from unauthorized access at all times.

5.1.1 Site Location and Construction

DigiCert performs its CA operations from secure and geographically diverse commercial data centers. The data centers are equipped with logical and physical controls that make DigiCert's CA operations inaccessible to non-trusted personnel as described in section 5.1.2. DigiCert operates under a security policy designed to detect, deter, and prevent unauthorized access to DigiCert's operations.

RA are expected to maintain the same levels of protection and requirements of the DirectTrust CP and describe those practices in their RPS if applicable.

5.1.2 Physical Access

DigiCert and RAs protect equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering.

For DigiCert, the secure parts of DigiCert CA hosting facilities are protected using physical access controls making them accessible only to appropriately authorized individuals in layers of security as described here. 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 in each subsequent area. 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.

Access to the data centers housing the CA 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 that specify which layers of security they have access to based on their trusted role status and designated responsibilities described in section 5.2.1.

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.

DigiCert personnel perform periodic security checks 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. RAs must maintain the same levels of protection as required by the DirectTrust CP if separate from DigiCert these will be described in the RPS if applicable.

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 systems are located on raised flooring, and the data centers are equipped with monitoring systems to detect excess moisture.

RA equipment is installed in such a way that it is not in danger of exposure to water other than water from fire prevention and protections systems.

5.1.5 Fire Prevention and Protection

No stipulation.

5.1.6 Media Storage

DigiCert protects its media from accidental damage and unauthorized physical access. Backup files are created on a regular basis. DigiCert's backup files are maintained at locations separate from DigiCert's primary data operations facility.

5.1.7 Waste Disposal

CA media and documentation that are no longer needed for operations are destroyed in a secure manner. All unnecessary copies of printed sensitive information are shredded on-site before disposal.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted Roles

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. 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 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 by DigiCert is maintained and reviewed annually. RAs may have different requirements for appointing trusted roles. The process used by RAs for appointing and governing Trusted Roles is specified in the applicable RPS.

The requirements of the DirectTrust program are defined in terms of four roles:

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

Some roles may be combined. The following subsections provide a detailed description of the responsibilities for each role.

5.2.1.1 Administrators

The administrator role is responsible for:

- Installation, configuration, and maintenance of the CA;
- Establishing and maintaining CA system accounts; and
- Configuring Certificate profiles or templates and audit parameters and generating and backing up CA keys.

Administrators do not issue Certificates to Subscribers.

5.2.1.2 Officers – Validation and Vetting Personnel

The officer role is responsible for issuing Certificates, that is:

- Registering new Subscribers and requesting the issuance of Certificates;
- Verifying the identity of Subscribers and accuracy of information included in Certificates; and
- Approving and executing the issuance of Certificates, and requesting, approving, and executing the revocation of Certificates.

5.2.1.3 Internal Auditors

The auditor role is responsible for:

- Reviewing, maintaining, and archiving audit logs; and

- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its CPS and this CP.

5.2.1.4 Operator

The operator role is responsible for the routine operation of the CA equipment and operations such as system backups and recovery or changing recording media.

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.

5.2.3 Identification and Authentication for each Role

All personnel are required to authenticate themselves to CA and RA systems before they are allowed access to systems necessary to perform their trusted roles.

External RA system access and control by trusted roles are specified in the respective RPS.

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 key management or CA administration.

Any individual may assume the Operator role.

No one individual can assume both the Officer and Administrator roles.

For RAs, the separation of duties for trusted roles are addressed in their respective RPS if applicable.

5.3 PERSONNEL CONTROLS

5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling Trusted Roles are selected on the basis of loyalty, trustworthiness, and integrity. The DCPA is responsible and accountable for DigiCert's PKI operations and ensures compliance with this CP/CPS. 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.

For Trusted Roles maintained by RAs external to DigiCert, these requirements will be addressed in their respective RPS.

5.3.2 Background Check Procedures

DigiCert and RAs verify 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.

For Trusted Roles maintained by RAs external to DigiCert, these requirements will be addressed in their respective RPS.

5.3.3 Training Requirements

Persons in a Trusted Roles receive comprehensive training in all aspects of the role they perform.

DigiCert provides skills training to all employees involved in DigiCert's PKI operations. The training relates to the person's job functions and covers basic Public Key Infrastructure (PKI) knowledge.

DigiCert maintains records of who received training and what level of training was completed where applicable.

5.3.4 Retraining Frequency and Requirements

Trusted roles 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 CP/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 must perform their duties as prescribed and are subject to sanctions stated above in Section 5.3.6. Otherwise, independent contractors and consultants are escorted and directly supervised by Trusted Persons when they are given access to DigiCert and any of its secure facilities.

5.3.8 Documentation Supplied to Personnel

Personnel in trusted roles are provided with the documentation necessary to perform their duties. 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.

For Trusted Roles maintained by RAs external to DigiCert, these requirements will be addressed in their respective RPS and will include the relevant CP, this CP/CPS, and technical specification documents.

5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for all events relating to the security of the CA. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

5.4.1 Types of Events Recorded

DigiCert's systems require identification and authentication at system logon with a unique username 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 applications in order to record the events listed below. If DigiCert's applications cannot automatically record an event, DigiCert or an RA implements manual procedures to satisfy the requirements. For each event, DigiCert records the relevant:

- date and time,
- type of event,
- success or failure, and
- user or system that caused the event or initiated the action.

Event records are available to auditors as proof of DigiCert's or RA practices.

Auditable Event	Auditable Event Details
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 unsuccessful authentication attempts reached 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	Any change to the trusted public keys, including additions and deletions
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, and renewal
	Certificate issuance
CERTIFICATE REVOCATION	All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION	
CA CONFIGURATION	Any security-relevant changes to the configuration of a CA system component
ACCOUNT ADMINISTRATION	Roles and users are added or deleted
	The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT	All changes to the certificate profile

REVOCATION PROFILE MANAGEMENT	All changes to the revocation profile
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT	All changes to the certificate revocation list profile
TIME STAMPING	A third-party time stamp is obtained
MISCELLANEOUS	Appointment of an individual to a Trusted Role
	Installation of an Operating System
	Installation of a PKI Application
	Installation of a Hardware Security Modules
	System Startup
	Logon attempts to PKI Application
	Attempts to set passwords
	Attempts to modify passwords
	Backup of the internal CA database
	Restoration from backup of the internal CA database
	All certificate compromise notification requests
	Zeroizing HSMs
	Re-key of the Component
CONFIGURATION CHANGES	Hardware
	Software
	Operating System
	Patches
PHYSICAL ACCESS / SITE SECURITY	Known or suspected violations of physical security
ANOMALIES	System crashes and hardware failures
	Software error conditions
	Software check integrity failures
	Network attacks (suspected or confirmed)
	Equipment failure
	Violations of a CP or CPS
	Resetting Operating System clock

In generally, DigiCert audits all activities related to the CA, including security events, authentication to systems, data entry, key generation, private key storage, etc. The systems audited are dependent on platform as well as requirements specified by the community of interest. Anomalies in the system are investigated and tracked.

5.4.2 Frequency of Processing Log

When checking logs, 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

Security audit log data is available on the CA equipment for a minimum of two months.

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 systems are configured to ensure that:

1. only authorized people have read access to logs,
2. only authorized people may archive audit logs, and
3. 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.

5.4.5 Audit Log Backup Procedures

Security audit data may be backed up at least monthly and stored off-site in a secure location.

5.4.6 Audit Collection System

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, External Program PMAs, and suspend 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

5.5.1 Types of Records Archived

DigiCert retain the following information in its archives (as such information pertains to DigiCert's CA operations in the CP and legal agreements):

1. Accreditations of DigiCert,
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. Rejection or acceptance of a certificate request,
6. Certificate issuance, re-key, 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. CRL and OCSP entries,
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 certificate status change 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/CPS.

5.5.2 Retention Period for Archive

CA archives are kept for a minimum of seven years & 6 months.

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.

5.5.4 Archive Backup Procedures

No stipulation.

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)

No stipulation.

5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

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, OCSP responses, 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.

If the old Private Key is used to sign CRLs that contain Certificates signed with that key, then the old key will be retained and protected.

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.

If a hacking attempt or other form of potential compromise of DigiCert becomes known, DigiCert shall investigate in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in Section 5.7.3 are followed. Otherwise the scope of potential damage is assessed in order to determine if the CA needs to be rebuilt, only some Certificates need to be revoked, and/or the CA key needs to be declared compromised.

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. DigiCert may generate a new key pair and sign a new certificate.

If a CA key is compromised, the trusted self-signed Certificate will be removed from each Relying Party application, and a new one distributed via secure out-of-band mechanisms.

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 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. 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.

5.8 CA OR RA TERMINATION

In the event of CA termination, Certificates signed by DigiCert will be revoked.

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key Pair Generation

6.1.1.2 CA Key Pair Generation

CA key pairs are generated by trusted roles and using a cryptographic hardware device. Typically, the cryptographic hardware is evaluated to FIPS 140-1 Level 3 and EAL 4+. Community requirements may specify a lower version of control. DigiCert creates auditable evidence during the key generation process to prove that the CP/CPS was followed and role separation was enforced during the key generation process.

6.1.1.3 Subscriber Key Pair Generation

Cryptographic key pairs for Subscriber Certificates are created on physical hardware that is well protected. The cryptographic module used for key generation are in accordance with section 6.2.1 of this CP/CPS.

6.1.2 Private Key Delivery to Subscriber

If Subscribers generate their own key pairs or there is no key delivery to Subscriber, then this section does not apply.

When DigiCert or a CA generate key pairs on behalf of the Subscriber, the private key is delivered securely to the Subscriber Private keys meeting the following requirements:

- Anyone who generates a private signing key for a Subscriber shall not retain any copy of the key after delivery of the private key to the Subscriber.
- The private key must be protected from activation, compromise, or modification during the delivery process.
- The Subscriber shall acknowledge receipt of the private key(s).
- Delivery shall be accomplished in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers.
- For hardware modules, accountability for the location and state of the module must be maintained until the Subscriber accepts possession of it.
- For electronic delivery of private keys, the key material shall be encrypted using a cryptographic algorithm and key size at least as strong as the private key. Activation data shall be delivered using a separate secure channel.
- For shared key applications, organizational identities, and network devices, see also Section 3.2 of this CP/CPS.

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. For DirectTrust LoA1 Certificates, no stipulation.

For DirectTrust LoA1 Certificates, no stipulation.

6.1.4 CA Public Key Delivery to Relying Parties

A new CA root Public Key will be delivered within a self-signed Certificate using a commercially reasonable out-of- band medium trusted by the relying party.

6.1.5 Key Sizes

DigiCert generates and use the following keys, signature algorithms, and hash algorithms for signing Certificates, CRLs, and Certificate status server responses:

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

DigiCert only issues end-entity Certificates that contain at least 2048-bit Public Keys for RSA, DSA, or Diffie- Hellman, or at least 224 bits for elliptic curve algorithms.

The DCPA may require higher bit keys in its sole discretion upon review of the DirectTrust Certificate Profiles.

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 and by the DirectTrust CP and DirectTrust Certificate Profile document.

Group Certificates cannot assert the contentCommitment bit.

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.

All Subscriber Certificates SHALL assert a Basic Constraint of CA:FALSE and may assert an extended key usage not in conflict with the Certificate primary key usages.

Subscriber Single-Use Certificates

A single-use Certificate is a Certificate intended for digital signing only, encryption only or Content Commitment only. A Subscriber key pair to be used for digital signing is bound to a

Certificate asserting only the digitalSignature key usage bit. A Subscriber key pair to be used for encryption only is bound to a Certificate asserting only the keyEncipherment key usage bit. A Subscriber key pair to be used for Content Commitment only is bound to a Certificate asserting both the contentCommitment key usage bit and the digitalSignature key usage bit. Content Commitment certificates cannot be used to sign the health container of a Direct Message.

Subscriber Dual-use Certificates
A dual-use Certificate is a Certificate intended for digital signing and/or encryption usage. A Subscriber key pair that is intended for both digital signing and encryption is bound to a Certificate asserting both the digitalSignature and keyEncipherment key usage bits.

Issuer CA Certificates
An Issuer CA Certificate SHALL assert the following key usage bits:

- cRLSign
- keyCertSign

Issuer CA Certificates SHALL assert a Basic Constraint of CA:TRUE.

6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules are expected to be validated to the FIPS PUB 140 minimum level as identified below for the relevant party (or provide an equivalent protection):

Entity	FIPS 140 Validation Level
CA	Level 2
RA	Level 1
Custodian (e.g. HISP)	Level 2[3]
Subscriber	Level 1

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

No Stipulation.

6.2.3 Private Key Escrow

DigiCert does not escrow Private Keys of Certificates.

6.2.4 Private Key Backup

DigiCert's CA Private Key is backed up to a secure offsite location to facilitate disaster recovery.

Subscriber Private Keys are not backed up.

[3] Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys are transferred from one cryptographic module to another to perform CA key backup procedures in section 6.3.4.

All other keys are generated by and in a cryptographic module. In the event that a private key is to be transported from one cryptographic module to another, the private key is encrypted during transport; private keys never exist in plaintext form outside the cryptographic module boundary.

6.2.7 Private Key Storage on Cryptographic Module

If private keys are stored in a cryptographic module, then the module is required to meet section 6.2.1 as applicable for the entity.

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.

DigiCert protects the activation data for their private keys against loss, theft, modification, disclosure, or unauthorized use.

CA administrators are authenticated to the cryptographic token before the activation of the associated private key(s). Entry of activation data is protected from disclosure (i.e., the data is not be displayed while it is entered).

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 or Custodians are required to authenticate themselves to the cryptographic module before activating their private keys. Authentication to the cryptographic module in order to activate the Private Key associated with a given certificate requires authentication commensurate with the AAL asserted in the certificate.

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. 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. 3 Custodial Subscriber Key Stores hold keys for a number of Subscriber certificates in one location.

6.2.10 Method of Destroying Private Keys

DigiCert/RA 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.

Subscriber signature Private Keys are destroyed when they are no longer needed or when the time period for the Private Key's use expires as specified in in 6.3.2.

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 CA Certificate and the associated Private Key are used for a maximum of 20 years.

Subscriber Private Keys are used for signing for a maximum period of 6 years.

Subscriber Certificates have a maximum lifetime of 3 years.

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. 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. If DigiCert uses passwords as activation data for a signing key, DigiCert will change the activation data change upon re-key of the CA Certificate.

If a Custodian or Subscriber uses passwords as activation data for a signing key, they are required to change the activation data upon rekey of the respective Certificate.

DigiCert only transmits activation data via an appropriately protected channel that is distinct in time and place from delivery to the associated cryptographic module.

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. DigiCert protects the activation data for its private keys using methods that protect against the loss, theft, modification, unauthorized disclosure, or unauthorized use of such private keys. These details are maintained in the disaster recovery procedures. DigiCert maintains an audit trail of Secret Shares, and Shareholders participate in the maintenance of an audit trail.

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation of Private Key for Content Commitment

For credentials that carry the Content Commitment bit, Subscribers are authenticated to the cryptographic module prior to activation of the Private Key prior to each digital signature. Authentication to the cryptographic module in order to activate the Private Key associated with a given certificates require authentication commensurate with the AAL asserted in the certificate.

6.4.3.2 Authentication for Private Key Activation

The Keystore Operator (e.g. Subscriber or Custodian) protects data used to unlock and activate Private Keys from disclosure using a combination of cryptographic and physical access control mechanisms appropriate for the Level of Authentication asserted in the Certificate.

The Custodian must only activate a Subscriber or End User's Private Key during a secure session that is protected at the same level as the protection mechanism required for the Private Key activation and during which the Subscriber or End User has authenticated at a level appropriate for the Private Key being protected and has proactively confirmed intent to authorize activation.

Authentication of a Subscriber or an End User for the purpose of unlocking and activating the Private Key is performed by verifying that the Subscriber or End User controls one or more Authenticators that are associated with that Subscriber or End User.

DirectTrust Levels of Authentication are intended to provide equivalent assurances to the Authenticator Assurance Levels (AALs) as defined by NIST SP 800-63-3 and as described in the "Guidance for Authentication of Individual Identity", a companion document to the DirectTrust CP and this CP/CPS. The following table defines the DirectTrust Levels of Authentication that may be asserted in a Certificate issued under this program and specific authentication requirements that must be met to be compliant when a given Level of Authentication is asserted:

Level of Authentication	Authentication Requirements
DirectTrust Auth AAL1	This level of authentication provides some assurance that the Subscriber or authorized End User controls an authenticator registered to the Subscriber or End User. Single-factor Authentication is required using a wide range of available authentication technologies. Successful authentication requires that the Subscriber or End User prove possession and control of the Authenticator(s) through a secure authentication protocol.
DirectTrust Auth AAL2	This level of authentication provides high confidence that the Subscriber or authorized End User controls an authenticator registered to the Subscriber or End User. Proof of possession and control of two different authentication factors is required through a secure authentication protocol and, when applicable, using approved cryptographic techniques.
DirectTrust Auth AAL3	This level of authentication provides very high confidence that the Subscriber or authorized End User controls an authenticator registered to the Subscriber or End User. Authentication is based on proof of possession of a key through a cryptographic protocol. A hardware-based cryptographic authenticator and an authenticator that provides verifier impersonation resistance is required.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific Computer Security Technical Requirements

Computer security controls are required to ensure CA operations are performed as configure its CA 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.

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.

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 responses, 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

All system clock time for DigiCert are derived from a trusted time service. Asserted times are accurate to within three minutes. Electronic or manual procedures may be used to maintain system time.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version Number(s)

All certificates are X.509 version 3 certificates.

DigiCert issues DirectTrust Certificates in accordance with approved DirectTrust Certificate Profiles corresponding to the DirectTrust CP.

7.1.2 Certificate Extensions

DigiCert uses standard Certificate extensions that are compliant with IETF RFC 5280. The Key Usage, Extended Key Usage, and Basic Constraints extensions are populated as specified in section 6.1.7 of the DirectTrust CP and this CP/CPS. The CRL Distribution Points extension may be populated with a CRL URL as specified in section 2.2 of this CP/CPS. The Authority Information Access extension maybe populated with an OCSP Responder location as specified in section 2.2.1. The Subject Alternative Name extension is populated as specified in section 3.1.1. The Certificate Policies extension are populated as defined in section 7.1.6.

7.1.3 Algorithm Object Identifiers

Algorithm object identifiers used by DigiCert are as follows:

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 uses the following OID for identifying the subject Public Key algorithm: rsaEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4 Name Forms

Name forms are specified in section 3.1.1.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

DigiCert asserts in the certificatePolicies extension of the Certificate an OID for each of the following categories in accordance with Section 1.2.

- The DirectTrust CP version under which DigiCert operates;
- The Level of Assurance at which the end entity was identity proofed; and
- The healthcare category.

A Certificate that asserts the keyUsage bit for Content Commitment asserts a DirectTrust

AAL OID. If the Certificate is issued to a Device, the Device Certificate OID is asserted.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation.

7.1.9 Processing Semantics for the Critical Certificate Policies Extension

DirectTrust does not require the certificatePolicies extension to be critical. Relying Parties whose client software does not process this extension risk using Certificates inappropriately.

7.2 CRL PROFILE

DigiCert generates CRLs in accordance with approved DirectTrust CRL profiles. See Section 7.1.

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	[As appropriate]
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

DigiCert complies with the CRL and CRL Extensions profile defined in IETF RFC 5280.

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	Required – select reason for revocation

DigiCert signs the CRL using the SHA-256 signature algorithm and identify it using the

following OID:

- sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}.

7.3 OCSP PROFILE

7.3.1 Version Number(s)

DigiCert's OCSP responders conform to version 1 of RFC 2560.

7.3.2 OCSP Extensions

Extensions are set in accordance with RFC 2560.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENT

8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

DigiCert undergo an audit of its compliance with the DirectTrust CP at least once every two years. Audits referencing this CP/CPS shall cover DigiCert's CA systems, Sub CAs, and OCSP Responders. RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS if applicable.

8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

DigiCert select auditors that demonstrate competence in the field of compliance audits. The CA compliance auditor must be thoroughly familiar with the requirements which the CA imposes on the issuance and management of its Certificates.

8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

The CA Declaration of Compliance describes the auditor's relationship to DigiCert, indicating whether the auditor is internal or an independent compliance auditor.

8.4 TOPICS COVERED BY ASSESSMENT

DigiCert will follow a DirectTrust accreditation program if provided. This program will certify the compliance of CAs, RAs, and Custodians (e.g. HISPs), in which case the program will outline the topics covered by assessment.

8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law, this CP/CPS, 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 and/or DirectTrust. The DCPA may require additional action if necessary to rectify any significant issues created by the non- compliance, including requiring revocation of affected certificates.

RAs must comply with the audit requirements as specified in the legal agreements, the CP, relevant technical specification requirements, and this CP/CPS. How those audit requirements are met will be stipulated in their RPS if applicable.

8.6 COMMUNICATION OF RESULTS

The results of each audit and declaration of compliance are reported to the DCPA and to the designated DirectTrust web page. DigiCert may elect to share the audit report results with other entities in its sole discretion.

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 in accordance with the applicable customer agreement.

9.1.2 Certificate Access Fees

If not specified in the relevant legal agreements or CP of an associated third party, 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

As set forth in the relevant customer agreement with DigiCert.

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

As set forth in the relevant legal agreements.

9.2.3 Insurance or Warranty Coverage for End-Entities

No stipulation.

9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1 Scope of Confidential Information

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

- Private Keys;

- Activation data used to access Private Keys or to gain access to the CA system;
- Business continuity, incident response, contingency, and disaster recovery plans;
- Other security practices used to protect the confidentiality, integrity, or availability of information; Information held by DigiCert as private information in accordance with Section 9.4;
- Audit logs and archive records; and
- Transaction records, financial audit records, and 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 CP/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. RAs are contractually required to protect 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. RAs may have a different standard of care as specified in their RPS if applicable.

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 CP/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.

All intellectual property of entities participating in the DigiCert Private PKI remains the property of its respective owners as per the relevant legal agreements.

9.6 REPRESENTATIONS AND WARRANTIES

9.6.1 CA Representations and Warranties

Except as expressly stated in this CP/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 CP/CPS, that:

DigiCert:

- DigiCert complies, in all material aspects, with this CP/CPS and all applicable laws and regulations,
- DigiCert publishes and updates CRLs and OCSP responses on a regular basis,
- Does not warrant the accuracy, authenticity, completeness, or fitness of any unverified information,
- Is not responsible for information contained in a certificate except as stated in this CP/CPS,
- Does not warrant the quality, function, or performance of any software or hardware device, and

- Is not responsible for failing to comply with this CP/CPS because of circumstances outside of DigiCert's control.

9.6.2 RA Representations and Warranties

RAs represent that:

1. The RA's certificate issuance and management services conform to this CP/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 CP/CPS. DigiCert's agreement with the RA may contain additional representations.

9.6.3 Subscriber Representations and Warranties

Subscribers are solely responsible for any misrepresentations they make to third parties and for all transactions that use the 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 and RAs,
3. Limit Users to only employees or Affiliates of the organization named in the Certificate Subject (for certificates listing an organization), to the Patient to whom the certificate is issued or representatives authorized by the Patient (for Patient Certificates), or to the individual Subscriber named in the Certificate Subject (for Content Commitment certificates);
4. Confirm the accuracy of the certificate data prior to using the certificate,
5. Promptly cease using a certificate and notify DigiCert if (i) any information that was submitted to DigiCert/the RA or is included in a certificate changed or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, this CP/CPS, the DirectTrust 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 CP/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 CP/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. A Relying Party shall use a DirectTrust Certificate for the purpose for which it was intended and check each Certificate for validity.

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 LIABILITY 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 CP/CPS IN PROVIDING THE CERTIFICATE OR SERVICE. Subscriber agreements and agreements

with relying parties may contain different limitations on liability, in which case the agreement controls.

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 CP/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 CP/CPS, or
v. whether any provision of this CP/CPS was proven ineffective.

The disclaimers and limitations on liabilities in this CP/CPS are fundamental terms to the use of DigiCert's certificates and services.

9.9 INDEMNITIES

9.9.1 Indemnification by DigiCert

As set forth in the relevant customer agreement.

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 CP/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 CP/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 CP/CPS and any amendments to the CP/CPS are effective when adopted by the DCPA and remain in effect until replaced with a newer version.

9.10.2. Termination

This CP/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 CP/CPS's termination via email or 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 agreements remain effective until the certificate is revoked or expired, even if this CP/CPS terminates.

9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

DigiCert accepts notices related to this CP/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 the relevant customer agreement.

9.12 AMENDMENTS

9.12.1 Procedure for Amendment

This CP/CPS is periodically reviewed and updated by the DCPA. Controls are in place to reasonably ensure that this CP/CPS is not amended and published without the prior authorization of the DCPA.

9.12.2 Notification Mechanism and Period

DigiCert does not guarantee or set a notice-and-comment period and may make changes to this CP/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 CP/CPS.

9.12.3 Circumstances under which OID Must Be Changed

The DCPA is solely responsible for determining whether an amendment to the CP/CPS requires an OID change upon the notification from DirectTrust and its PMA.

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 laws of the state of Utah govern the interpretation, construction, and enforcement of this CP/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 CP/CPS or any DigiCert product or service.

9.15 COMPLIANCE WITH APPLICABLE LAW

This CP/CPS is subject to all applicable laws and regulations, including United States restrictions on the export of software and cryptography products.

9.16 MISCELLANEOUS PROVISIONS

9.16.1 Entire Agreement

DigiCert contractually obligates any entity operating under this CP/CPS to comply with this CP/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 CP/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 CP/CPS may not assign their rights or obligations without the prior written consent of DigiCert. Unless specified otherwise in a contract with a party, DigiCert does not provide notice of assignment.

9.16.3 Severability

If any provision of this CP/CPS is held invalid or unenforceable by a competent court or tribunal, the remainder of the CP/CPS will remain valid and enforceable. Each provision of this CP/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 CP/CPS does not waive DigiCert's right to enforce the same provision later or right to enforce any other provision of this CP/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 CP/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. Clauses for force majeure will be added to the extent of applicable law for relevant parties and affiliates within the associated legal agreements.

9.17 OTHER PROVISIONS

No stipulation unless otherwise specified in the relevant legal agreements.