DirectTrust Community
X.509 Certificate Policy

Current Version: Version 2.0

October 7, 2020

DirectTrust Community
X.509 Certificate Policy v2.0 Approvals

- October 7, 2020

Revision History

Document Version	Document Date	Revision Details
2.0	October 7, 2020	Extensive changes to Section 3, Section 6 and other sections to support NIST 800-63-3 IALs, add support for Content Commitment certificates and clarify requirements for Patient Certificates. Other minor clarifications made throughout.
1.4 with erratum	December 10. 2018	Erratum for Section 6.2.1 to clarify allowable validation for cryptographic modules. Erratum for Section 6.2.7 to clarify applicability requirements for private key storage.
1.4	June 27, 2018	Section 3.2 modified to include requirements for verification of NPI numbers, if included in Certificates. Other minor clarifications made throughout.
1.3 with erratum	December 7, 2016	Erratum to correct Section 6.2.1
1.3 with errata	December 1, 2016	Errata to correct name of DirectTrust-EHNAC Accreditation programs.
1.3	August 10, 2016	Section 1.2 and other sections modified to require assertion of category OIDs. Added new policy OID for Device Certificates. Added new language for effective date and EOL regarding previous CP versions. Section 3.2.2 clarified regarding vetting requirements for healthcare category OIDs. Section 6.1.7 clarified regarding

		allowance of separate signing and encryption Certificates. Section 6.1.5 modified to disallow obsolete hash algorithms and bring into alignment with Section 7 requirements. Definitions and terms clarified, including usage of defined terms throughout. Some sections previously in Section 1 moved to Introduction to bring CP into better alignment with RFC 3647. Numerous changes made to improve flow and readability.
1.2.1	October 17, 2014	Incorporated accumulated errata and clarifying text that do not require reassignment of the CP policy OIDs. Extensive changes were made within Section 3.2.
1.2	January 18, 2013	Added descriptions of Certificate types with multiple assurance levels mapping to NIST 800-63-2. Expanded multiple sections to be more in line with other communities of interest and baseline CA operations at FBCA Basic.
1.1	December 9, 2011	Consensus of Workgroup reached to modifications.
0.9, 1.0	September 23, 2011	Addressed conformance with FBCA. Consensus approved by WG - the consensus voting page can be found here <http://wiki.directproject.org/Direct+Ecosystem+Community+Consensus+Statement+-+August+4%2C+2011>
0.8	September 16, 2011	Updated with DirectTrust governance content
0.7	August 26, 2011	Removed references to DNS
0.6	August 22, 2011	Changes based on comments received during consensus process
0.5	August 3, 2011	Add OCSP option and fix remaining CPS references

0.4	July 28, 2011	Changes based on wiki discussion threads
0.3	July 23, 2011	Changes based on 7/22/2011 workgroup call
0.2	July 13, 2011	Small changes (typos).
0.1	July 13, 2011	Initial draft.

Contents

1 Introduction

DirectTrust.org, Inc. (DirectTrust) is a non-profit and competitively neutral entity operated by and for participants in the Direct community and other communities involved in electronic health information exchange that benefit from leveraging a healthcare-centric PKI. The establishment of DirectTrust was anticipated in the Direct Ecosystem Community Certificate Policy Version 0.9. The DirectTrust Board of Directors is responsible for approval of this CP and for overseeing the compliance of DirectTrust member CA practices with this CP.

The Public Key Infrastructure (PKI) to which this CP applies supports applications that includes secure exchange of electronic information by Covered Entities, Business Associates, Healthcare Entities, Consumer/Patients, Non-Declared Entities; IHE query-based transactions; FHIR and other specifications, including those grounded in the specification of the Direct Project.

The Direct Project developed the original Direct Ecosystem Community Certificate Policy Version 0.9 in accordance with its consensus process. The Direct Project is an initiative sponsored by the Office of the National Coordinator (ONC) for Health Information Technology to allow participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. The Direct Project is based on S/MIME message signatures and message encryption for the purposes of achieving privacy, authentication, and message integrity.

This DirectTrust Community Certificate Policy (hereafter CP) modifies the original Direct Ecosystem Community Certificate Policy Version 0.9 so that it can be referenced in all digital Certificates in compliance with this CP. This CP also provides a set of policies under which compliant CAs may publish their related Certification Practices Statement and attest to their compliance with this CP.

This CP is intended to be fully consistent with US Federal Government requirements for identity proofing as described in NIST Special Publication (SP) 800-63-2 or 800-63-3. More specifically, identity proofing levels of assurance defined in this CP are intended to align with NIST SP 800-63-2 or 800-63-3 identity proofing levels of assurance. However, this CP also specifies requirements that further constrain the conditions under which a DirectTrust Community compliant digital Certificate may be issued, utilized, and managed.

Operational requirements for issuing Certification Authorities and Registration Authorities operating under this CP are intended to be, at a minimum, consistent with operational requirements defined in the U.S. Federal Bridge Certification Authority CP for an entity operating at a Basic assurance level.

This DirectTrust Community X.509 Certificate Policy (CP) follows the structure of the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure (PKI) Certificate Policy and Certification Practices Framework (RFC 3647). Pursuant to the IETF PKIX RFC 3647 CP/CPS framework, this CP is divided into nine parts that cover the security controls and practices and procedures for Certificate and related services within the PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

1.1 Overview

This DirectTrust Community X.509 Certificate Policy (DirectTrust CP) describes the unified policy under which a compliant Certification Authority operates. 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.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119. The elements of this CP specified by MUST, MUST NOT, REQUIRED, SHALL, and SHALL NOT constitute required elements. The elements in this CP specified by SHOULD, SHOULD NOT, and RECOMMENDED are not mandatory, but represent consensus of DirectTrust members on recommended best practices. In the event a best practice conflicts with a required element, the required element applies. The elements in this CP specified by MAY and OPTIONAL are not recommendations. Some of these elements reflect operational aspects that are not necessarily performed by CAs or RAs, or there may be disagreement among DirectTrust members as to whether or not these elements represent best practices, but some number of DirectTrust members agree with their inclusion.

1.1.1 Certificate Policy (CP)

The effective date of this CP v2.0 is upon approval by the DirectTrust Board of Directors. CP v1.4 and CP v1.4 with errata will EOL on October 7, 2021 (one year from the effective date of this CP v2.0). Issuer CAs SHALL operate in compliance with this CP v2.0 or later within one year from the effective date.

Digital Certificates that comply to this CP MUST 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 this CP, an OID corresponding to an identity proofing Level of Assurance (LoA), and an OID corresponding to a healthcare category SHALL be

available to Relying Parties. An Issuing CA MUST assert the appropriate OIDs in the *certificatePolicies* extension of Certificates.

1.1.2 Relationship between this DirectTrust CP and a Corresponding CPS

DirectTrust may publish a Certification Practices Statement (CPS) showing how it supports establishment of compliance to this CP. Alternatively, it may establish and document procedures to support the publishing of a declaration of compliance by CAs issuing digital Certificates complying with the requirements of this CP. DirectTrust supports an accreditation program to certify a compliant CPS and the operations and policies of its CA to the standards outlined by the accreditation program.

1.1.3 Relationship between this DirectTrust CP and the CA CP

A compliant CA MAY assert a mapping between its CP and this DirectTrust CP in the *policyMappings* extension of its CA Certificate.

1.1.4 Relationship between DirectTrust CP and DirectTrust Accredited Entities

Compliance to an Active CP Version is a requirement for accreditation under the DirectTrust Accreditation Program as described in CP Section 1.5.3, and entities accredited under this program have been 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.

Practice Note: A Relying Party may also encounter DirectTrust policy OIDs in Certificates issued by or used by non-accredited entities claiming compliance with this CP. The assertion of a DirectTrust policy OID in a Certificate, in and of itself, does not imply that the Custodian (e.g. HISP), CA, or RA has been accredited by the DirectTrust Accreditation Program or is a member of DirectTrust, or that the issuer of the certificate has complied with the requirements of this CP regarding the use of any DirectTrust policy OID.

1.2 Document Name and Identification

This 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 CP 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)]

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

id-DirectTrust. arc		**1.3.6.1.4.1.41179**
id-DirectTrust-policies	**id-DirectTrust.(0)**	**1.3.6.1.4.1.41179.0**
DirectTrust-CP 2.0	id-DirectTrust-policies.(2.0)	1.3.6.1.4.1.41179.0.2.0
id-DirectTrust-LoAs	**id-DirectTrust.(1)**	**1.3.6.1.4.1.41179.1**
DirectTrust ID LoA 1	id-DirectTrust-LoAs.(1)	1.3.6.1.4.1.41179.1.1
DirectTrust ID LoA 2	id-DirectTrust-LoAs.(2)	1.3.6.1.4.1.41179.1.2
DirectTrust ID LoA 3	id-DirectTrust-LoAs.(3)	1.3.6.1.4.1.41179.1.3
DirectTrust ID LoA 4	id-DirectTrust-LoAs.(4)	1.3.6.1.4.1.41179.1.4
DirectTrust ID IAL 1	id-DirectTrust-LoAs.(1)	1.3.6.1.4.1.41179.1.1
DirectTrust ID IAL 2	id-DirectTrust-LoAs.(5)	1.3.6.1.4.1.41179.1.5
DirectTrust ID IAL 3	id-DirectTrust-LoAs.(6)	1.3.6.1.4.1.41179.1.6
Note: DirectTrust LoA1 and DirectTrust IAL 1 are interchangeable and equivalent and therefore have the same OID.		
id-DirectTrust-Cat	**id-DirectTrust.(2)**	**1.3.6.1.4.1.41179.2**
DirectTrust CE	id-DirectTrust-Cat.(1)	1.3.6.1.4.1.41179.2.1
DirectTrust BA	id-DirectTrust-Cat.(2)	1.3.6.1.4.1.41179.2.2
DirectTrust HE	id-DirectTrust-Cat.(3)	1.3.6.1.4.1.41179.2.3
DirectTrust Patient	id-DirectTrust-Cat.(4)	1.3.6.1.4.1.41179.2.4
DirectTrust Non-Declared	id-DirectTrust-Cat.(5)	1.3.6.1.4.1.41179.2.5
id-DirectTrust-Dev	**id-DirectTrust.(3)**	**1.3.6.1.4.1.41179.3**
DirectTrust Device	id-DirectTrust-Dev.(1)	1.3.6.1.4.1.41179.3.1

id-DirectTrust-auth-LoAs	**id-DirectTrust.(6)**	**1.3.6.1.4.1.41179.6**
DirectTrust Auth AAL 1	id-DirectTrust-auth-LoAs (5)	1.3.6.1.4.1.41179.6.5
DirectTrust Auth AAL 2	id-DirectTrust-auth-LoAs (6)	1.3.6.1.4.1.41179.6.6
DirectTrust Auth AAL 3	id-DirectTrust-auth-LoAs (7)	1.3.6.1.4.1.41179.6.7
id-DirectTrust-Cont	**id-DirectTrust.(7)**	**1.3.6.1.4.1.41179.7**
DirectTrust Content Commitment	id-DirectTrust-Cont.(1)	1.3.6.1.4.1.41179.7.1

Issuers CAs SHALL assert only the OIDs above when issuing under the DirectTrust arc. Policy OIDs asserting additional compliance with other CPs, i.e. under a different policy arc MAY be asserted.

NOTE: The Direct Project specification does not explicitly require utilization of policy OIDs as a mechanism of asserting trust. Rather a set of trust anchor Certificates is maintained by a relying party and each presented Certificate MUST chain to a Certificate within this set of trust anchor Certificates. HISPs that provide services partitioned in accordance with DirectTrust policy OIDs MAY maintain and publish a collection of trust anchor Certificates (a "bundle") from compliant CAs, each referencing a common set of policy OIDs, that the relying party MAY include in its set of trust anchor Certificates. This requires that Issuer CAs that comply to the DirectTrust profiles ONLY issue Direct Certificates and indicate which policy OIDs the CA issues Certificates for, in order to be effectively utilized by Subscribers to HISPs that depend exclusively upon binary trust of CA Certificates. A Trust Bundle for a given set of policy OIDs will only include CA Certificates whose minimum issuance capability is equivalent to the Trust Bundle LoA e.g. if a CA is capable of issuing both Level 2 and Level 3 Direct Certificates, then it will only be included in Level 2 Trust Bundles since that is the only LoA that it can guarantee at a minimum in terms of Certificates issued by it. HISPs that support interrogation of Certificates to find LoA (e.g. via policy OID) will have greater flexibility in configuring Trust Bundles.

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

1.3 PKI Participants

PKI Participants are those entities involved in the registration, issuance, use of, or reliance upon DirectTrust Certificates. The following are descriptions of each Participant.

Compliance with this CP alone may be insufficient for DirectTrust accreditation and/or acceptance into DirectTrust trust anchor bundles. Please contact DirectTrust for more information.

1.3.1 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 this CP are hereafter referred to as "Issuer CAs". CAs accredited by DirectTrust or DirectTrust-EHNAC for DirectTrust issuance operate under a Certification Practices Statement (CPS) that is reviewed as part of the accreditation process to ensure compliance to the policies of this CP.

1.3.2 Registration Authorities (RAs)

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. The requirements in this CP apply to all RAs operating under this CP. Although DirectTrust RAs are accredited by DirectTrust or DirectTrust-EHNAC, an issuing CA relying on an RA different than the CA MUST monitor RA's compliance with this policy, the Issuer CA CPS, and if applicable, any Registration Practices Statement (RPS) under which the RA operates. An Issuer CA accredited for DirectTrust issuance SHALL only rely on RAs that are accredited as RAs by DirectTrust or DirectTrust-EHNAC to operate in compliance with this CP and the accredited CA's CPS and approved by the DirectTrust Policy Committee (DTPC).

1.3.2.1. Trusted Agents

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

The CA or RA MAY provide the Trusted Agent with material to facilitate the activities being performed by the Trusted Agent on behalf of the CA or 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 SHALL be performed in accordance with this CP, the applicable CA CPS, and any applicable RA RPS.

Practice Note: A "Trusted Agent" as defined in this CP is not synonymous with "Trusted Agent" as defined in DirectTrust or *DirectTrust-EHNAC accreditation documents.*

1.3.3 Subscribers

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.

Prior to proofing of identity and issuance of a certificate, a Subscriber is an Applicant.

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 Providers (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.

Practice Note: Custodians (including HISPs) may be subject to additional requirements regarding management of Private Keys for DirectTrust accreditation and/or acceptance into DirectTrust trust anchor bundles.

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 the CA and RA to register the above elements in accordance with Section 3.2.2 and 3.2.3 and is responsible for meeting the obligations of Subscribers as defined throughout this document.

1.3.4 Relying Parties

A Relying Party uses 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

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 SHOULD evaluate the application environment and associated risks before deciding whether to accept a Certificate issued under this CP for any particular purpose.

An Affiliate that is a healthcare provider or healthcare organization SHALL 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 SHALL only be an Affiliate of another Covered Entity and SHALL NOT 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) SHALL 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, or 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 to a known level of assurance when the Certificate was issued. Certificates issued under this policy may not be used where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The DirectTrust Board of Directors or such other entity as it may designate is responsible for managing and facilitating a process for approval, administration and interpretation of this document that is aligned with the practices and procedures of the Direct Project.

1.5.2 Contact Person

Questions regarding this CP should be directed to:

DirectTrust.org, Inc.

E-mail: Admin@DirectTrust.org

Mail: 1629 K. Street NW, Suite 300, Washington, DC 20006

Web: https://www.directtrust.org/

1.5.3 Person Determining Certification Practices Statement Suitability

The CPS of a CA defines the certification practices and operating controls utilized by the CA. Each CA operating under this CP is responsible for ensuring and asserting that their CP and/or CPS as applicable is in compliance with this DirectTrust CP. The CA CPS MUST designate the person or organization authorized to make these assertions.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronym	Meaning
BA	Business Associate
CA	Certification Authority
CE	Covered Entity
CFR	Code of Federal Regulations
CP	Certificate Policy
CPS	Certification Practices Statement

CRL	Certificate Revocation List
DN	Distinguished Name
DTPC	DirectTrust Policy Committee
FHIR	Fast Healthcare Interoperability Resources (HL7)
HE	Healthcare Entity
HISP	Healthcare Information Services Provider
ID	Identity Document
IdM	Identity Management
IETF	Internet Engineering Task Force
IHE	Integrating the Healthcare Enterprise
ISSO	Information System Security Officer
LoA	Level of Assurance
OCSP	Online Certificate Status Protocol
OID	Object Identifier
ONC	Office of the National Coordinator for Health Information Technology
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request for Comments
S/MIME	Secure Multipurpose Internet Mail Extensions
TA	Trusted Agent

1.6.2 Definitions

Term	Definition
Activation Data	Private data, other than cryptographic keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events).
Address-Bound Certificate	An Address-Bound Certificate is a Certificate that contains a full Direct Address in the form of an RFC 822 email address in the Certificate Subject Alternative Name extension.
Affiliate	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. See section 1.3.5.1.
Affiliated Organization	An Affiliated Organization is an entity that authorizes organizational affiliation with the Subscriber of a Certificate.
Applicant	An Applicant is a person or other legal entity that submits an application and identifying information to the CA or RA for the purpose of obtaining or renewing a Certificate.
Authenticator Assurance Level (AAL)	A category describing the strength of the authentication process.
Business Associate	A Business Associate (BA) helps Covered Entities carry out health care activities and functions under a written business associate contract or other arrangement with the Business Associate that establishes specifically what the Business Associate has been engaged to do and requires the Business Associate to comply with the requirements to protect the privacy and security of protected health information. Business Associates in this CP are as defined under HIPAA at 45 CFR 160.103.
Certificate	A Certificate is a x.509-compliant digital representation of information that at least (1) identifies the Certification Authority

	issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's Public Key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it.
Certification Authority	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. See section 1.3.1.
Certificate Policy	A Certificate Policy (CP) is a specialized form of administrative policy tuned to electronic transactions performed during Certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital Certificates.
Certification Practices Statement	A Certification Practices Statement (CPS) is a statement of the practices that a CA employs in issuing, suspending, revoking, and renewing Certificates and providing revocation status to Relying Parties.
Certificate Revocation List	A Certificate Revocation List (CRL) is a list maintained by a Certification Authority of the Certificates which it has issued that are suspended or revoked prior to their stated expiration date.
Code of Federal Regulations	The Code of Federal Regulations (CFR) are regulations imposed by U.S. Federal law.
Content Commitment	A Content Commitment Certificate is used for verifying digital signatures which are intended to signal that the signer is committing in some way to the content being signed. The type of commitment the certificate can be used to support may be further constrained by the issuing CA, e.g. through a certificatePolicies extension entry. The precise type of commitment of the signer e.g. "reviewed and approved" or "with the intent to be bound" may be constrained by certificatePolicies extension entries or may be signaled by the content being signed, e.g. the signed document itself or some additional signed information. Certificates intended to be used for Content Commitment will have both the *contentCommitment* and *digitalSignature* keyUsage bits set. Note: The *contentCommitment* bit was previously known as the *nonRepudiation* bit.

Covered Entity	A Covered Entity (CE) is an individual, organization, or agency that protects the privacy and security of health information and provides individuals with certain rights with respect to their health information. Covered Entities in this CP are as defined under HIPAA at 45 CFR 160.103.
Cryptographic Module	The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms.
Custodial Subscriber Key Store	A Custodial Subscriber Key Store holds keys for a number of Subscriber Certificates in one location.
Device	A Device is a non-human system component. Examples of Devices include but are not limited to routers, firewalls, servers, imaging systems, consumer diagnostics, cameras, software components and other devices capable of securely handling Private Keys and properly implementing PKI technologies, either directly or through a Custodian (e.g. HISP when used for Direct messaging).
Device Certificate	A Device Certificate is a Certificate Issued to a Device.
Direct Address	A Direct Address consists of a Health Endpoint Name and a Health Domain Name concatenated with the "@" symbol. Examples: johndoe@direct.sunnyfamilypractice.example.org, er@direct.hospital.org
Direct Project	The Direct Project is an initiative from the Office of the National Coordinator (ONC) for Health Information Technology that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Domain-Bound Certificate	A Domain-Bound Certificate is a Certificate that contains a Health Domain Name in the form of a *dNSName* in the *subjectCommonName* and *subjectAlternativeName* extensions of the Certificate.

Healthcare Entity	A Healthcare Entity (HE) is an entity involved in healthcare, that has agreed to protect private and confidential patient information consistent with the requirements of HIPAA although it is not a Covered Entity or Business Associate as defined under HIPAA at 45 CFR 160.103
Health Domain Name	A Health Domain Name is a string conforming to the requirements of RFC 1034. *Example:* direct.sunnyfamilypractice.example.org. A Health Domain Name must be a fully qualified domain name and should be dedicated solely to the purposes of health information exchange.
Health Endpoint Name	A Health Endpoint Name is a string conforming to the local-part requirements of RFC 5322. Health Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. Example: johndoe (referring to in individual), sunnyfamilypractice, memoriallab (referring to organizational inboxes), diseaseregistry (referring to a processing queue).
Internet Engineering Task Force	The Internet Engineering Task Force (IETF) is a standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
Identity Assurance Level (IAL)	A category that conveys the degree of confidence that the Applicant's claimed identity is their real identity.
Information System Security Officer	An individual responsible for ensuring control of the Private Key of a group certificate.
Issuer or Issuing CA	An Issuer CA is a CA issuing Certificates in compliance with this CP.
Keystore Operator	The entity responsible for the protection of the Private Key (e.g. for encryption, decryption, or digital signing) of a Subscriber held in a

	Cryptographic Module. A Custodian is a Keystore Operator, and a Subscriber may be a Keystore Operator.
Level of Assurance	Level of Assurance (LoA) is the identity proofing level of assurance implemented for issuance of a Certificate. LoAs as used in this CP are intended to correspond to identity proofing levels of assurance as defined in NIST SP 800-63-2 or NIST SP 800-63-3.
Level of Authentication	Level of authentication specified via OID within a Certificate and which must be satisfied prior to any activation of the Private Key associated with the Certificate. Levels of Authentication as used in this CP are intended to align with the Authenticator Assurance Levels (AALs) as defined in NIST SP 800-63-3.
National Provider Identifier	A National Provider Identifier (NPI) is a unique 10-digit identification number issued by the Centers for Medicare and Medicaid Services (CMS).
Non-Declared Entity	A Non-Declared Entity is an entity that 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 / Consumer.
Non-Declared Entity Certificate	A Non-Declared Entity Certificate is a Certificate issued to a Non-Declared Entity.
Non-Repudiation	See Content Commitment definition.
Patient	A Patient is an individual using their Direct Address for exchange other than as a health care professional, Business Associate or individual associated with a HIPAA covered entity.
Patient Certificate	A Patient Certificate asserts a Patient OID in an Address Certificate issued to a Patient containing a full Direct Address in the form of an RFC 822 email address in the Certificate subjectAlternativeName extension. See section 1.2.

Private Key	A Private Key is the key of an asymmetric key pair kept secret by its holder, used to create Digital Signatures or to decrypt data encrypted with the holder's corresponding Public Key.
Public Key	A Public Key is the key of an asymmetric key pair publicly disclosed by the holder of the corresponding Private Key in the form of a Certificate. The Public Key is used for validation of a digital signature and encryption of data.
Public Key Infrastructure	Public Key Infrastructure (PKI) is a set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and Public-Private Key pairs, including the ability to issue, maintain, and revoke Public Key Certificates.
Registration Authority	A Registration Authority is an organization that is responsible for collecting and proofing a Subscriber's identity and verifying any other information provided by Subscriber for inclusion in a Certificate. See section 1.3.2.
Relying Party	A person or Entity who has received information that includes a Certificate and a digital signature verifiable with reference to a Public Key listed in the Certificate and is in a position to rely on them.
Sponsor	A Sponsor fills the role of a Subscriber for non-human system components named as Public Key Certificate Subjects. The Sponsor works with the CA and RA to register the above elements in accordance with Section 3.2.2 and 3.2.3 and is responsible for meeting the obligations of Subscribers as defined throughout this document.
Subscriber	A Subscriber is an entity that either (1) authorized application for the certificate, or (2) is the subject named or identified in a certificate issued to that entity. A Subscriber holds, directly or through its designated HISP (or other Subscriber-authorized third party), a Private Key that corresponds to the Public Key listed in the Certificate.
Trust Bundle	A Trust Bundle is a collection of CA Certificates used as trust anchors by a Relying Party.

Trusted Agent	An entity authorized to act as a representative in confirming the Subscriber's identity during the registration process as specified in Section 1.3.2.1.
Trusted Role	A Trusted Role is held by individuals performing functions that are fundamental to the integrity of the PKI.
User	A User is a natural person or Device authorized by a Subscriber to access or make use of the Private Key corresponding to the Subscriber's Certificate.

2 Publication and Repository Responsibilities

2.1 Repositories

Issuer CAs and RAs SHALL operate repositories in support of operations required by this CP and related CPS. At a minimum, an Issuer CA SHALL ensure that its root Certificate and the revocation data for issued Certificates are available through a repository.

2.1.1 Repository Obligations

Repositories holding Certificate status data SHOULD be operated 24 hours a day, 7 days a week with a minimum of 99% availability overall per year.

2.2 Publication of Certification Information

2.2.1 Publication of Certificates and Certificate Status

Each Issuer CA SHALL maintain a Certificate Revocation List (CRL) and expose its location in the CRL distribution points X.509v3 extension. An Issuer CA MAY also choose to maintain an equivalent Online Certificate Status Protocol (OCSP) Responder and expose its location in the Authority Information Access extension of the Certificate. If a CA maintains an OCSP Responder, it MUST do so in accordance with the relevant requirements in sections 4.9 and 7.3.

CA and end entity Certificates SHALL only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties. Each Issuer CA MUST publish its CA Certificate and any other intermediate or trust anchor Certificates necessary to validate the Issuer CA.

2.2.2 Publication of CA Information

Each Issuer CA SHALL publish information concerning the CA necessary to support its operation and use. Information on how to obtain a copy of this CP SHALL be provided to any party with legitimate interest. Issuer CAs MAY choose to publish their CPS in its entirety or make available a redacted version.

2.2.3 Interoperability

No stipulation.

2.3 Frequency of Publication

This CP and any ensuing changes SHALL be made available within 14 days of approval by DirectTrust.

2.4 Access Controls on Repositories

Issuer CAs and RAs SHALL protect repository information not intended for public dissemination or modification. Issuer CAs SHALL provide unrestricted read access to its repositories for legitimate uses and SHALL implement logical and physical controls to prevent unauthorized write access to such repositories.

3 Identification and Authentication

3.1 Naming

3.1.1 Types of Names

All Certificates SHALL use non-null DN name forms for the issuer and subject names.

Address-Bound Certificates contain a full Direct Address in the form of an RFC 822Name 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

Names used in Certificates SHALL uniquely identify the subject of the Certificate and SHALL be easily understood by humans.

3.1.3 Anonymity or Pseudonymity of Subscribers

CAs SHALL NOT issue anonymous Certificates. Pseudonymous Certificates MAY be issued as long as name space uniqueness requirements are met.

3.1.4 Rules for Interpreting Various Name Forms

No stipulation.

3.1.5 Uniqueness of Names

CAs SHALL enforce name uniqueness of the Certificate subject DN within the CA's X.500 namespace.

3.1.6 Recognition, Authentication, and Role of Trademarks

Subscribers SHALL NOT request Certificates with any content that infringes the intellectual property rights of another entity. Issuer CAs MAY reject any application or require revocation of any Certificate that is part of a trademark dispute.

3.2 Initial Identity Validation

3.2.1 Method to Prove Possession of Private Key

In the case where the Private Key is generated by the CA, no proof of Private Key possession is required. In the case where the Subscriber generates its own Private Key, then the Subscriber MUST digitally sign a known piece of data with the Private Key and send it to the Issuer CA. The Issuer CA will verify the signature and the known piece of data thus proving Private Key possession.

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 MUST 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 3.1.1 for details).

The requesting organization MUST represent 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, MUST be a legally distinct entity. If a domain name or email address (RFC 822 name) is asserted in the Certificate, then the Subscriber MUST have the right to use it.
For all Certificates asserting an organization name, the Issuer CA or the RA SHALL verify the organization and the organization's category in accordance with the following minimum requirements. The organization's category OID SHALL be asserted in all Certificates.

Healthcare Category	**Minimum Verification Requirements**
DirectTrust CE	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. *The RA shall verify 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.
DirectTrust BA	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. *The RA shall verify 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.*
DirectTrust HE	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. *The RA shall verify 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.*
DirectTrust Non-Declared	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. *The RA shall verify 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, the RA SHALL 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.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

Identity proofing is REQUIRED for an individual acting as a:

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

DirectTrust Levels of Assurance 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, the Issuer CA or the RA SHALL proof an individual's identity in accordance with one of the following assurance levels:

DirectTrust LoA 1	The name associated with the Applicant is provided by the Applicant and accepted without verification. *The RA verifies Applicant's control over an email address (or any of the identity proofing methods listed for a higher level).*
DirectTrust LoA 2	Applicant supplies full legal name, an address of record, and date of birth. **In-Person Vetting** For in-person vetting, the Applicant also provides valid government issued photo ID. *The RA inspects the photo-ID; compares picture to Applicant; and records the ID number, address, and date of birth (DoB)* *The CA issues 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.*

	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. *The 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).* *The CA issues 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	Applicant supplies full legal name, an address of record, and date of birth. **In-Person Vetting** For in-person vetting, the Applicant also provides a valid government issued photo ID. *The 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. *The CA issues 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, CA also records Applicant's voice or uses alternative means that establish an equivalent level of non-repudiation.* **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. *The 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).* *The CA issues 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.

DirectTrust IAL2	Applicant supplies his or her full legal name, an address of record and date of birth of their claimed identity. **In-Person Vetting** 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 SHALL be confirmed as genuine by 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 SHALL be 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".* *The CA issues 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.* **Remote Vetting** (unsupervised) 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 SHALL be confirmed as genuine by 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 SHALL be 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."* *The CA 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, the CA 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 destination address of record for the enrollment code unless that destination was a postal address.
DirectTrust IAL 3	Applicant supplies his or her full legal name, an address of record and date of birth of their claimed identity. **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 SHALL be confirmed as genuine by 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 SHALL be 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 is provided in the "Guidance for Authentication of Individual Identity".* *The CA 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.* *CA issues certificate and delivers it in a secure manner to the appropriate Subscriber.* **Remote Vetting** *Remote Vetting is not permitted.*

Practice Note: Knowledge-based Verification "KBV" has a limited role in IAL2 identity proofing as discussed in the "Guidance for Authentication of Individual Identity." For example, The CSP SHALL NOT use KBV questions for which the answers do not change (e.g., "What was your first car?"). This is a ***significant*** *change from LoA2 and LoA3, and CA/RAs that are currently using KBV for identity validation and verification for LOA3 may not be able to use the same approach they do now.*

Any government issued ID provided by the Applicant that includes an expiration date MUST be 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.

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.

Practice Note: At the time this CP 2.0 was published, the assertion of IAL 2 was optional under the DirectTrust Accredited Trust Anchor Bundle (ATAB). It was anticipated that most Certificates intended to meet the ATAB requirements under this CP 2.0 would assert the LoA 3 OID or both the LoA3 OID and the IAL 2 OID—a Relying Party requiring IAL 2 or higher should confirm that the proper OID has been asserted.

For Patient Certificates, the Issuer CA or the RA SHALL proof the Patient identity in accordance with any of the above LoA requirements, collect the Subscriber Representation, and SHALL assert in the Certificate the DirectTrust Patient OID and the appropriate LoA OID.

DirectTrust Patient	**Subscriber Representation** Applicant represents that the Certificate applied for will be used for health information exchange purposes. *The RA verifies that the Applicant has made this representation.*

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

Role based Certificates are considered Group Certificates under this CP 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.

For Custodian-managed Certificates, an Issuer CA or RA SHALL 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 SHALL also be performed:

- The Custodian ISSO or equivalent SHALL be 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 MUST be 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 MUST 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 MUST be made available by the Subscriber Organization to the RA upon request.

Practice Note: The Subscriber may be able to leverage its existing relationship as an employer or affiliate of a User to meet the identity verification requirements. For example, Federal Employment Eligibility Verification Form I-9 may be sufficient, either alone or with supplemental verification of submitted information to meet Level of Assurance requirements.

3.2.3.4 Authentication of Devices

An Issuer CA MAY issue a Certificate for use on or by a Device. In such cases, the Device MUST 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 SHALL also include 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 SHALL review the status of each Device to ensure it is still authorized to receive Certificates. The CPS of an Issuer CA SHALL describe procedures to ensure that Certificate accountability is maintained.

Practice Note: A Subscriber may authorize a Device under the control of the Subscriber to make use of its Certificate.

3.2.3.5 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 are 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 MUST be verified against the NPI Registry provided by the Centers for Medicare & Medicaid Services (CMS). The RA

MUST utilize 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 SHALL NOT be included in a Certificate.

3.2.5 Validation of Authority

Reference Section 3.2.2.

3.2.6 Criteria for Interoperation

This CP defines the criteria for issuance of Certificates interoperable within the DirectTrust community. These Certificates may additionally be relied upon by entities outside of the DirectTrust community.

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routine Re-key

The identity of an organization and/or individual requesting a re-key of a DirectTrust Certificate MUST be established through the initial identity proofing process or through proof of possession of the Private Key via a digital signature.

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 SHALL go through the initial identity proofing process described in section 3.2 to obtain a new Certificate.

3.4 Identification and Authentication for Revocation Request

Revocation requests MUST be authenticated. Requests to revoke a Certificate MAY be authenticated using that Certificate's Public Key, regardless of whether or not the associated Private Key has been compromised.

4 Certificate Life-Cycle

4.1 Application

This section specifies requirements for the initial application for a DirectTrust Certificate.

4.1.1 Submission of Certificate Application

A compliant Custodian (e.g. HISP) or Subscriber creates the Certificate Signing Request (CSR) based on input received from the Subscriber as validated by the RA or CA during the identity proofing process.

4.1.2 Enrollment Process and Responsibilities

A Subscriber is responsible for providing accurate information about himself and his organization during identity proofing. The Issuer CA is responsible for ensuring that the identity of each Applicant is proofed in accordance with this CP and the applicable CPS prior to the issuance of a Certificate. The Issuer CA and RA SHALL authenticate and protect all communication made during the Certificate application process.

4.2 Certificate Application Processing

The Issuer CA and RA are responsible for verifying that the information in a CSR is accurate and reflect the information presented by the Subscriber.

4.2.1 Performing Identification and Authentication Functions

The identity proofing of Subscribers SHALL be done by the Issuer CA or RA as specified in section 3.2 using procedures detailed in the applicable CPS or RPS.

4.2.2 Approval or Rejection of Certificate Applications

A Certificate application MAY be rejected by an Issuer CA or RA due to missing or inaccurate information. Each Issuer CA or RA retains the right to reject Certificate applications if, in its judgment, the requesting individual or organization has not provided sufficient information for issuance.

4.2.3 Time to Process Certification Applications

No stipulation.

4.3 Issuance

4.3.1 CA Actions During Certificate Issuance

The Issuer CA SHALL verify the source of a certificate request before issuance. The Issuer CA SHALL ensure that all Certificate fields and extensions are properly populated.

4.3.2 Notification to Subscriber of Certificate Issuance

The Subscriber MUST be notified via physical mail, or email or an equivalent means that the Certificate has been issued.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

Failure to object to the certificate or its contents, or actual use of the Certificate, constitutes the Subscriber's acceptance of the certificate.

4.4.2 Publication of the Certificate by the CA

CA certificates SHALL be published as specified in 2.2.1. This specification makes no stipulation regarding publication of Subscriber certificates.

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 their authorized Custodian (e.g. HISP) representatives, who take possession of their Private Key, SHALL protect it from access by unauthorized parties and SHALL use the Private Keys only as specified by the *certificatePolicies, keyUsage* and *extKeyUsage* extensions of the corresponding Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Certificates SHALL comply with the policies provided by this CP. Relying Parties SHOULD understand these policies. The Issuer CA MUST publish a CRL and/or maintain an OCSP Responder. Relying Parties SHOULD process the CRL on a regular basis and reject Certificates found on it and/or respect the Certificate status reflected in an OCSP response.

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 MUST NOT be further re-keyed, renewed, or modified.

4.6.1 Circumstance for Certificate Renewal

A Certificate MAY be renewed if the Public Key has not reached the end of its validity period, the associated Private Key has not been compromised, and the Subscriber name and attributes are unchanged. Certificates MAY also be renewed if the compliant DirectTrust CA re-keys.

4.6.2 Who May Request Renewal

The Issuer CA MAY request renewal of its own Certificate. For Subscriber Certificates, the Subscriber or their authorized representative, or the RA MAY request renewal.

4.6.3 Processing Certificate Renewal Requests

The Issuer CA or RA SHALL approve or reject Subscriber Certificate renewal requests. Identity proofing of the Subscriber SHALL be equivalent to the initial identity proofing process or executed via proof of possession of the Private Key through a digital signature.

4.6.5 Conduct Constituting Acceptance of a Renewed Certificate

Failure to object to the renewed Certificate or its contents, or actual use of the Certificate, constitutes the Subscriber's acceptance of the Certificate.

4.6.6 Publication of the Renewal Certificate by the CA

The Issuer CA or other entities MAY publish Subscriber Certificates in a directory specified in section 2.2.1.

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 MUST NOT be further re-keyed, renewed, or modified.

4.7.1 Circumstance for Certificate Re-Key

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

4.7.2 Who May Request Certification of a New Public Key

An Issuer CA, the RA, the Subscriber or their authorized representative MAY request the re-key of a Subscriber Certificate.

4.7.3 Processing Certificate Re-Keying Requests

The Issuer CA or RA SHALL approve or reject Subscriber Certificate re-keying requests. Identity proofing of the Subscriber SHALL be 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 New Certificate Issuance 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 Re-keyed 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 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 MUST NOT be further re-keyed, renewed, or modified. Whether or not the old Certificate is required to be revoked SHALL be determined in accordance with section 4.9.

4.8.1 Circumstance for Certificate Modification

A Certificate MAY be modified if some of the information in the Certificate has changed.

4.8.2 Who May Request Certificate Modification

The Subscriber or their authorized representative or the RA MAY request modification of a Subscriber Certificate.

4.8.3 Processing Certificate Modification Requests

Identity proofing for a Certificate modification request SHALL be accomplished 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 New Certificate Issuance to Subscriber

See section 4.3.2.

4.8.5 Conduct Constituting Acceptance of 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 Issuance by the CA to Other Entities

See section 4.4.3.

4.9 Certificate Revocation and Suspension

4.9.1 Circumstances for Revocation

A Certificate SHALL 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.

Whenever any of the above circumstances occur, the associated Certificate SHALL be revoked and placed on the CRL and, when applicable, have its revoked status reflected in OCSP responses.

4.9.2 Who Can Request Revocation

The Subscriber, an authorized representative, the RA, or the CA MAY request revocation of a Certificate.

4.9.3 Procedure for Revocation Request

Any request for Certificate revocation, other than a request from the CA or Subscriber, SHALL identify the Certificate to be revoked by serial number and explain the reason for revocation. An Issuer CA or RA SHALL ensure that the Certificate revocation request is not malicious and will verify that the reason for revocation is valid.

If the reason for revocation is valid or the request originates from the Subscriber, the Issuer CA SHALL revoke the Certificate and place the Certificate's serial number and any other REQUIRED 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 this policy. Subscribers and other participants SHALL 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

An Issuer CA MUST process all revocation requests within 8 hours of receipt. CRL issuance frequency is addressed in Section 4.9.7.

4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

Practice Note: Use of revoked Certificates could have damaging or catastrophic consequences. Relying Parties should consider the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed. It is recommended Relying Parties obtain revocation data in real time. A cached CRL should not be relied upon for more than 24 hours or beyond the time specified in the CRL next Update field, whichever occurs first.

4.9.7 CRL Issuance Frequency

An Issuer CA MUST issue 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 SHALL be no more than 31 days after the CRL is published.

The Issuer CA MUST ensure that superseded CRLs are removed from the public repository upon posting of the latest CRL.

4.9.8 Maximum Latency of CRLs

CRLs SHALL be posted within four hours after generation. Furthermore, a new CRL SHALL be 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

A CA MAY deploy an Online Certificate Status Protocol (OCSP) responder.

4.9.10 On-Line Revocation Checking Requirements

No stipulation.

4.9.11 Other Forms of Revocation Advertisements Available

No other form of revocation advertisement is REQUIRED.

4.9.12 Special Requirements Related to Key Compromise

In the event of a CA Private Key compromise or loss, a CRL shall be published at the earliest feasible time. When a CA certificate is revoked or Subscriber Certificate is revoked because of compromise or suspected compromise of a Private Key, a CRL must be issued within 18 hours of notification.

4.9.13 Circumstances for Suspension

Certificate suspension occurs by marking a Certificate as revoked with a reason code of “On Hold.” These Certificates SHALL be placed on the next CRL and SHALL remain

on the CRL until the Certificate is restored or the Certificate expires. A Certificate is restored when the CA reinstates it. Certificates that are marked as revoked with a reason code other than "On Hold" SHALL NOT be restored. Issuer CAs are not REQUIRED to support suspended Certificates, but MAY opt to do so.

4.9.14 Who Can Requests Suspension

No stipulation.

4.9.15 Procedure for Suspension Request

No stipulation.

4.9.16 Limits on Suspension Period

No stipulation.

4.10 Certificate Status Services

Issuer CAs MAY support Certificate status services beyond a CRL (OCSP).

4.10.1 Operational Characteristics

No stipulation.

4.10.2 Service Availability

No stipulation.

4.10.3 Optional Features

No stipulation.

4.11 End of Subscription

Certificates that have expired prior to or upon end of subscription are not REQUIRED to be revoked. 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 his Certificate revoked.

4.12 Key Escrow and Recovery

No stipulation.

4.12.1 Key Escrow and Recovery Policy and Practices

No stipulation.

4.12.2 Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5 Facility Management and Operations Controls

5.1 Physical Controls

Issuer CA and RA equipment SHALL be protected from unauthorized access at all times.

5.1.1 Site Location and Construction

The location and construction of the facility housing CA/RA equipment SHALL be consistent with facilities used to house sensitive information. The location and construction SHALL provide robust protection against unauthorized access to the CA/RA equipment and records.

5.1.2 Physical Access

The CA/RA equipment SHALL always be protected from unauthorized access with appropriate access control. Entry SHALL be restricted to trained CA Officers only.

5.1.3 Power and Air Conditioning

The CA/RA equipment SHALL possess a UPS to allow for a graceful shutdown in the event of power failure. Should excessive heat build-up occur in the physical surroundings of the CA equipment, procedures SHALL be in place to prevent equipment damage.

5.1.4 Water Exposures

CA/RA equipment SHALL be installed such 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

CA/RA media SHALL be stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information SHALL be duplicated and stored in a location separate from the CA/RA equipment and SHALL be protected from unauthorized access.

5.1.7 Waste Disposal

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

5.2 Procedural Controls

5.2.1 Trusted Roles

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

The requirements of this policy are defined in terms of four roles:

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 Administrator

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 Officer

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 Auditor

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

At least two people are trained for each task but only one is required to execute each task.

5.2.3 Identification and Authentication for Each Role

A person occupying a Trusted Role SHALL authenticate himself to the CA system.

5.2.4 Separation of Roles

Any individual MAY assume the Operator role. No one individual SHALL assume both the Officer and Administrator roles.

5.3 Personnel Controls

5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling Trusted Roles SHALL be selected on the basis of loyalty, trustworthiness, and integrity. All Trusted Roles are REQUIRED to be held by persons who are legally eligible to work in the United States.

5.3.2 Background Check Procedures

No stipulation.

5.3.3 Training Requirements

Persons in a Trusted Role SHALL receive comprehensive training in all aspects of the role they perform. All persons SHALL have a reasonable understanding of PKI principles and operations.

5.3.4 Retraining Frequency and Requirements

Individuals responsible for Trusted Roles SHALL be aware of changes in CA operation. Any significant change to the operations SHALL have a training (awareness) plan, and the execution of such plan SHALL be documented. Documentation SHALL be maintained identifying all personnel who received training and the level of training completed.

5.3.5 Job Rotation Frequency and Sequence

No stipulation.

5.3.6 Sanctions for Unauthorized Actions

Issuer CAs SHALL take appropriate administrative and disciplinary actions against any personnel or contractors who violate this policy.

5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the CA SHALL meet the personnel requirements set forth in this CP.

5.3.8 Documentation Supplied to Personnel

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

5.4 Audit Logging Procedures

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

5.4.1 Types of Events Recorded

A message from any source received by the Issuer CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record SHALL include the following (either recorded automatically or manually for each auditable event):

- The type of event;

- The date and time the event occurred;
- A success or failure indicator, and where appropriate
- The identity of the entity and/or operator (of the Issuer CA) that caused the event.

Detailed audit requirements are listed in the table below. All security auditing capabilities of the Issuer CA operating system and CA applications required by this CP SHALL be enabled. As a result, most of the events identified in the table SHALL be automatically recorded. Where events cannot be automatically recorded, the CA SHALL implement manual procedures to satisfy this requirement.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of 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

5.4.2 Frequency of Processing Log

Audit logs are reviewed and monitored regularly to ensure that any irregularities are identified and handled properly.

5.4.3 Retention Period for Audit Logs

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

5.4.4 Protection of Audit Logs

Only authorized personnel (CA officers) SHALL have access to the logs, and only authorized personnel SHALL archive the logs. CA configuration and processes SHALL enforce these requirements.

5.4.5 Audit Log Backup Procedures

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

5.4.6 Audit Collection System (internal vs. external)

All security audit processes SHALL be invoked at CA startup and cease only at shutdown. SHOULD it become apparent that an automated security audit system has failed, the CA SHALL cease all operation except for revocation processing until the security audit capability can be restored.

5.4.7 Notification to Event-Causing Subject

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

5.4.8 Vulnerability Assessments

The CA SHALL be subjected to the same vulnerability assessments as other critical systems.

5.5 Records Archival

5.5.1 Types of Events Archived

Issuer CA archive records SHALL be sufficiently detailed as to verify that the CA was properly operated as well as verify the validity of any Certificate throughout its validity period. At a minimum, the following data SHALL be archived:

- Any accreditation of the Issuer CA;
- CP and CPS versions;
- Contractual obligations and other agreements concerning the operation of the CA;
- System and equipment configurations, modifications, and updates;
- Certificate and revocation requests;
- Identity authentication data;
- Any documentation related to the receipt or acceptance of a Certificate or token;
- Subscriber Agreements;
- Issued Certificates;
- A record of Certificate re-keys,

- CRLs,
- Any data or applications necessary to verify an archive's contents,
- Compliance auditor reports,
- Any changes to the Issuer CA's audit parameters,
- Any attempt to delete or modify audit logs,
- Key generation (excluding session keys),
- Access to Private Keys for key recovery purposes,
- Changes to trusted Public Keys,
- Export of Private Keys,
- Approval or rejection of a Certificate status change request,
- Appointment of an individual to a Trusted Role,
- Destruction of a cryptographic module,
- Certificate compromise notifications,
- Remedial action taken as a result of violations of physical security, and
- Violations of the CP or CPS.

5.5.2 Retention Period for Archive

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

5.5.3 Protection of Archive

Only authorized individuals SHALL be permitted to add to or delete from the archive. Archive media SHALL be stored in a separate, safe, secure storage facility.

5.5.4 Archive Backup Procedures

No stipulation.

5.5.5 Requirements for Time-Stamping of Records

CA archive records SHALL be automatically time-stamped using a trusted time service, as they are created.

5.5.6 Archive Collection System (Internal vs. External)

No stipulation.

5.5.7 Procedures to Obtain & Verify Archive Information

No stipulation.

5.6 Key Changeover

The Issuer CA SHALL NOT issue Subscriber Certificates that extend beyond the expiration date of its own CA Certificates and Public Keys, and the CA Certificate

validity period MUST extend one Subscriber Certificate validity period past the last use of the CA Private Key. To minimize risk to the PKI through compromise of a CA's key, the CA Private Key will be changed more frequently, and only the new key will be used for Certificate signing purposes from that time. The older, but still valid, Certificate will be available to verify old signatures until all of the Subscriber Certificates signed under it have also expired. If the old Private Key is used to sign CRLs that contain Certificates signed with that key, then the old key MUST be retained and protected.

5.7 Compromise and Disaster Recovery

5.7.1 Incident and Compromise Handling Procedures

If a hacking attempt or other form of potential compromise of an Issuer CA becomes known, the Issuer CA 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 SHALL be followed. Otherwise the scope of potential damage SHALL be 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

Issuer CAs SHALL maintain backup copies of system, databases, and Private Keys in order to rebuild the CA capability in case of software and/or data corruption. Prior to resuming operations, the CA SHALL ensure that the system's integrity has been restored.

5.7.3 Entity Private Key Compromise Procedures

If a CA key is compromised, the trusted self-signed Certificate MUST 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

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations SHALL be reestablished as quickly as possible, giving priority to the ability to revoke Subscriber's Certificates. If the CA cannot reestablish revocation capabilities prior to the next update field in the latest CRL issued by the CA, then the CA governing body SHALL decide whether to declare the CA private signing key as compromised, and reestablish the CA keys and Certificates and all Subscriber Certificates, or allow additional time for reestablishment of the CA's revocation capability.

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, the CA will be completely rebuilt by reestablishing the CA equipment and generating new key pairs. Finally, all Subscriber Certificates SHALL be re-issued. In such events, any Relying Parties who continue to use Certificates signed with the destroyed Private Key do so at their own risk and the risk of others to whom they forward data.

5.8 CA and RA Termination

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

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

6.1.1.1 CA Key Pair Generation

The CA cryptographic keying material used to sign Certificates or CRLs SHALL be generated on physical hardware that is well protected. The cryptomodule used for key generation SHALL be in accordance with section 6.2.1 of this CP.

6.1.1.2 Subscriber Key Pair Generation

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

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 CAs or RAs generate keys on behalf of and for delivery to the Subscriber, then the private key MUST be delivered securely to the Subscriber. Private keys may be delivered electronically or may be delivered on a hardware cryptographic module. In all cases, the following requirements MUST be met:

- 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.

6.1.3 Public Key Delivery to CA

Where key pairs are generated by the Subscriber or RA, the public key and the Subscriber's identity must be delivered securely to the CA for Certificate issuance.

The delivery mechanism shall bind the Subscriber's verified identity to the public key. If cryptography is used to achieve this binding, it must be at least as strong as the CA keys used to sign the Certificate.

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

The Issuer CA SHALL generate 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)

The Issuer CA SHALL only issue 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 Issuer CA MAY require higher bit keys in its sole discretion.
DirectTrust Certificate Profiles may further constrain the requirements described in this Section.

6.1.6 Public Key Parameters Generation and Quality Checking

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

6.1.7 Key Usage Purposes

DirectTrust Certificate Profiles may further constrain the requirements described in this section.

Subscriber Certificates

All Subscriber Certificates SHALL assert key usages based on the intended application of the key pair.

Group Certificates SHALL NOT assert the contentCommitment 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 SHALL be bound to a Certificate asserting only the *digitalSignature* key usage bit. A Subscriber key pair to be used for encryption only SHALL be bound to a Certificate asserting only the *keyEncipherment* key usage bit. A Subscriber key pair to be used for Content Commitment only SHALL be bound to a Certificate asserting both the *contentCommitment* key usage bit and the *digitalSignature* key usage bit. Content Commitment certificates SHALL NOT 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 SHALL be 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 SHOULD 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
Subscriber	Level 1

6.2.1.1 Custodial Subscriber Key Stores

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

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

No stipulation.

6.2.3 Private Key Escrow

The Issuer CA SHALL NOT escrow Private Keys of Certificates that assert a key usage of *digitalSignature*. The Issuer CA MAY escrow Subscriber Private Keys used for encryption in order to provide key recovery as described in section 4.12.1.

6.2.4 Private Key Backup

The Issuer CA Private Key SHALL be backed up to a secure offsite location to facilitate disaster recovery.

Subscriber Private Keys MAY be backed up to a secure offsite location to facilitate disaster recovery.

6.2.5 Private Key Archival

No stipulation.

6.2.6 Private Key Transfer into or from a Cryptographic Module

Private Keys MAY be transferred only into a cryptographic module meeting the requirements of section 6.2.1 as applicable for the entity. Private keys SHALL NOT exist in the clear outside of a cryptographic module.

6.2.7 Private Key Storage on Cryptographic Module

If private keys are stored in a cryptographic module, then the module MUST meet the requirements of section 6.2.1 as applicable for the entity.

6.2.8 Method of Activating Private Keys

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

The Subscriber or Custodian must be authenticated to the cryptographic module before the activation of any Private Key(s). Authentication to the cryptographic module in order to activate the Private Key associated with a given certificate SHALL require authentication commensurate with the AAL asserted in the certificate.

6.2.9 Methods of Deactivating Private Keys

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

6.2.10 Method of Destroying Private Keys

Individuals in Trusted Roles SHALL destroy Private Keys when they are no longer needed. Subscriber signature Private Keys SHALL be 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 Management

6.3.1 Public Key Archival

Public keys are archived as part of the Certificate archival process.

6.3.2 Certificate Operational Periods/Key Usage Periods

An Issuer CA Certificate and the associated Private Key SHALL be used for a maximum of 20 years. Subscriber Private Keys SHALL be used for signing for a maximum period of 6 years. Subscriber Certificates SHALL have a maximum lifetime of 3 years.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The Issuer CA, Subscriber or a Custodian acting on behalf of the Subscriber SHALL generate activation data that has sufficient strength to protect its respective Private Keys. If the Issuer CA, Custodian or Subscriber uses passwords as activation data for a signing key, they SHALL change the activation data upon rekey of the respective Certificate. The Issuer SHALL only transmit 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

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

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

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

6.4.3 Other Aspects of Activation Data

6.4.3.1 Activation of Private Key for Content Commitment

For credentials that carry the Content Commitment bit, Subscribers SHALL be 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 certificate SHALL 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) SHALL protect 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 this CP. The following table defines the DirectTrust Levels of Authentication that may be asserted in a Certificate issued under this CP 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 are required.

6.5 Computer Security Controls

6.5.1 Specific Computer Security Technical Requirements

The Issuer CA SHALL 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.

The Issuer CA SHALL authenticate and protect all communications between individuals in Trusted Roles and its CA system.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

Issuer CA software SHALL be developed in a controlled development environment with modern source code control. Issuer CA hardware and software SHALL be dedicated to performing the CA tasks. Issuer CA hardware and software containing Private Keys SHALL be well protected. Hardware and software updates SHALL be tested and installed in a professional and controlled manner.

6.6.2 Security Management Controls

The configuration of an Issuer CA system as well as any modifications and upgrades SHALL be documented and controlled. A formal configuration management methodology SHALL be used for installation and ongoing maintenance of the Issuer CA system.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Information to be transferred from the Issuer CA SHALL be done through dedicated removable media or secure networks. The RA SHALL employ appropriate security

measures to ensure it is guarded against denial of service and intrusion attacks. Such measures include the use of guards, firewalls, and filtering routers.

6.8 Time Stamping

All system clock time for the Issuer CA system SHALL be derived from a trusted time service. Asserted times SHALL be accurate to within three minutes.

7 Certificate, CRL, and OCSP Profiles Format

7.1 Certificate Profile

DirectTrust publishes definitive and authoritative Certificate Profiles that may further constrain the requirements described in this Section. Certificate Profiles are versioned similar to this Certificate Policy version. As an example, Certificate Policy version X.Y. will have DirectTrust Certificate Profiles versioned X.Y.1, X.Y.2, X.Y.3, etc. Issuer CAs SHALL issue Certificates in accordance with approved DirectTrust Certificate Profiles corresponding to this CP version.

7.1.1 Version Numbers

A compliant Issuer CA SHALL issue X.509 v3 Certificates, which means the version field SHALL contain the integer 2.

7.1.2 Certificate Extensions

A CA SHALL use standard Certificate extensions that are compliant with IETF RFC 5280. The Key Usage, Extended Key Usage, and Basic Constraints extensions SHALL be populated as specified in section 6.1.7 of this CP. The CRL Distribution Points extension MAY be populated with a CRL URL as specified in section 2.2. The Authority Information Access extension MAY be populated with an OCSP Responder location as specified in section 2.2.1. The Subject Alternative Name extension SHALL be populated as specified in section 3.1.1. The Certificate Policies extension SHALL be populated as defined in section 7.1.6.

7.1.3 Algorithm Object Identifiers

End entity Certificates signed by an Issuer CA SHALL use 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}

An Issuer CA SHALL use 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

See section 3.1.1 of this Certificate Policy.

7.1.5 Name Constraints

No stipulation.

7.1.6 Certificate Policy Object Identifier

Issuer CAs MUST assert in the *certificatePolicies* extension of the Certificate an OID for each of the following categories in accordance with Section 1.2.

- The CP version under which the CA 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 SHALL assert a DirectTrust AAL OID.
- If the Certificate is issued to a Device, the Device Certificate OID MUST be 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 Policy Extension

This policy 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

Issuer CAs SHALL generate CRLs in accordance with approved CRL profiles. See Section 7.1.

7.2.1 Version Numbers

An Issuer CA SHALL issue X.509 version 2 CRLs, which means the version field SHALL contain the integer 1.

7.2.2 CRL and CRL Entry Extensions

An Issuer CA SHALL comply with the CRL and CRL Extensions profile defined in IETF RFC 5280.

An Issuer CA SHALL sign 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}.

The CRL SHALL contain a CRL Reason Code entry extension for each entry.

7.3 OCSP Profile

An Issuer CA MAY deploy an OCSP responder. See Section 7.1.

8 Compliance Audits and Other Assessments

Issuer CAs and RAs SHALL have a compliance audit mechanism in place to ensure that the requirements of this CP, the Issuer CA CPS and RPS (if applicable) are being implemented and enforced. This specification does not impose a requirement for any particular audit assessment methodology—it MAY be an internal audit process, or it MAY use a compliance auditor that is independent from the entity being audited.

DirectTrust SHALL provide a means for an Issuer CA to make a self-attested, legally binding declaration of compliance to this CP or a CA CP mapped to this CP and the related CPS. DirectTrust may provide an accreditation program to certify the compliance of CAs, RAs, and Custodians (e.g. HISPs), that includes the aforementioned attestation that the various entities will be audited against.

8.1 Frequency and Circumstances of Assessment

Issuing CAs and RAs MUST undergo an audit of its compliance with this CP at least once every two years. DirectTrust may provide an accreditation program to certify the compliance of Issuing CAs, RAs, and Custodians (e.g. HISPs), in which case the program will outline the requirements in respect to assessments.

8.2 Identity/Qualifications of Assessor

The auditor MUST 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. DirectTrust may provide an accreditation program to certify the compliance of CAs, RAs, and Custodians (e.g. HISPs), in which case the program will outline the requirements in respect to identity and qualifications of assessors.

8.3 Auditor’s Relationship to Assessed Entity

The CA Declaration of Compliance SHALL describe the auditor’s relationship to the CA, indicating whether the auditor is internal to the CA or an independent compliance auditor. DirectTrust may provide an accreditation program to certify the compliance of CAs, RAs, and Custodians (e.g. HISPs), in which case the program will outline the requirements in respect to the relationship of assessors to the assessed.

8.4 Topics Covered by Assessment

DirectTrust may provide an accreditation program to 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

CAs are not granted the right to claim compliance with reference to this CP unless they are in full compliance with the provisions and requirements of the CP. DirectTrust may take such steps as it deems appropriate to limit inaccurate claims of compliance. This may include limiting access to publications and other services of DirectTrust, loss of any accreditation status previously obtained, and DirectTrust may maintain a public discussion forum to discuss compliance issues.

8.6 Communication of Results

DirectTrust SHALL provide a web page or other appropriate means for CAs to report the status/results of the compliance assessment and audit process or to reference a location where such reports are available.

DirectTrust SHALL provide a web page or other appropriate means for CAs to publish their declaration of compliance or to reference a location where the declaration of compliance is available.

9 Other Business and Legal Matters

9.1 Fees

9.1.1 Certificate Issuance/Renewal Fees

No stipulation.

9.1.2 Certificate Access Fees

No stipulation.

9.1.3 Revocation or Status Information Access Fee

No stipulation.

9.1.4 Fees for other Services

No stipulation.

9.1.5 Refund Policy

No stipulation.

9.2 Financial Responsibility

9.2.1 Insurance Coverage

No stipulation.

9.2.2 Other Assets

No stipulation.

9.2.3 Insurance/Warranty Coverage for End-Entities

No stipulation.

9.3 Confidentiality of Business Information

9.3.1 Scope of Confidential Information

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

9.3.2 Information not within the scope of Confidential Information

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

9.3.3 Responsibility to Protect Confidential Information

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

9.4 Privacy of Personal Information

9.4.1 Privacy Plan

All identifying information for a Subscriber SHALL be protected from unauthorized disclosure. Issuer CAs SHALL create and follow a publicly posted privacy policy that specifies how the Issuer CA handles personal information.

9.4.2 Information Treated as Private

Information deemed as private SHALL be defined as such in agreements between the CA and its Subscribers.

Information included in Certificates is not deemed private.

9.4.4 Responsibility to Protect Private Information

An Issuer CA SHALL store private information securely.

9.4.5 Notice and Consent to Use Private Information

An Issuer CA SHALL use private information as dictated by the agreements with its Subscribers.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

An Issuer CA SHALL NOT disclose private information unless allowed by agreements with its Subscribers or unless REQUIRED to by law.

9.4.7 Other Information Disclosure Circumstances

No stipulation.

9.5 Intellectual Property Rights

DirectTrust and Issuer CAs will not knowingly violate the intellectual property rights held by others.

9.6 Representations and Warranties

9.6.1 CA Representations and Warranties

Issuer CAs MUST represent to DirectTrust, Subscribers, and Relying Parties that they comply, in all material aspects, with this CP, their CPS, and all applicable laws and regulations.

9.6.2 RA Representations and Warranties

At a minimum, Issuer CAs SHALL require RAs operating on their behalf to represent that they have followed this CP and the relevant CPS (or a qualifying RPS) when participating in the issuance and management of Certificates.

9.6.3 Subscriber Representations and Warranties

Each Subscriber SHALL represent to the Issuer CA that the Subscriber will:

1. Protect its Private Keys from compromise (including if a Custodian or HISP is employed who uses secure processes against potential compromise);
2. 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 to representatives authorized by the Patient (for Patient Certificates), or to the individual Subscriber named in the Certificate Subject (for Content Commitment certificates);
3. Provide accurate and complete information and communication to the Issuer CA and RA;
4. Confirm the accuracy of Certificate data prior to using the Certificate;
5. Promptly cease using a Certificate and notify the Issuer CA if (i) any information that was submitted to the Issuer CA or is included in a Certificate changes or becomes misleading, or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the Certificate;
6. Use the Certificate only for authorized and legal purposes, consistent with the relevant CPS and Subscriber Agreement, (including only installing Device Certificates on servers accessible at the domain listed in the Certificate); and
7. Promptly cease using the Certificate and related Private Key after the Certificate’s expiration.

9.6.4 Relying Parties Representations and Warranties

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 Affiliated Organizations

No stipulation.

9.6.6 Representations and Warranties of Other Participants

No stipulation.

9.7 Disclaimers of Warranties

No stipulation.

9.8 Limitations of Liabilities

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

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This CP becomes effective when approved through the DirectTrust consensus process and the DirectTrust Policy Committee. This CP has no specified term.

9.10.2 Termination

Termination of this CP may occur if approved through the DirectTrust consensus process.

9.10.3 Effect of Termination and Survival

The requirements of this CP remain in effect through the end of the archive period of the last Certificate issued.

9.11 Individual Notices and Communications with Participants

No stipulation.

9.12 Amendments

9.12.1 Procedure for Amendment

This CP may be amended through the DirectTrust consensus process. New CP versions are subject to approval by the DirectTrust Board.

9.12.2 Notification Mechanism and Period

CAs are notified of a change in the CP by DirectTrust posting an updated version of the CP to the DirectTrust website. Effective date and required dates for compliance are as stated in Section 1.2.

9.12.3 Circumstances Under Which OID Must be Changed

If a change in Certificate policy is deemed by DirectTrust to be substantive, a Certificate policy OID MUST be changed. New OIDs may be introduced or existing OIDs modified or removed with publication of a new CP version.

9.13 Dispute Resolution Provisions

Parties are required to notify DirectTrust and attempt to resolve disputes directly with DirectTrust before resorting to any dispute resolution mechanism, including adjudication or any type of alternative dispute resolution.

9.14 Governing Law

The laws of the United States of America SHALL govern this Policy.

9.15 Compliance with Applicable Law

All PKI participants SHALL comply with applicable laws.

9.16 Miscellaneous Provisions

9.16.1 Entire Agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If a court of competent jurisdiction determines that any provision of this CP is invalid or unenforceable, all other provisions of this CP SHALL remain in effect.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.