DirectTrust Community
X.509 Certificate Policy

Current Version: Version 1.2, January 25, 2013

Consensus approved by WG on V1.1 12/9/2011.

Revision History

Document Version	Document Date	Revision Details
1.2	January 18, 2013	Added descriptions of certificate types with multiple assurance levels mapping to NIST 800-63. 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

This Direct Trust 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).

The PKI to which this CP applies supports entities and applications involved in the exchange of electronic messages grounded in the specification of the Direct Project. 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, message integrity, and non-repudiation.

This CP is intended to be fully consistent with the Federal Bridge Certificate Authority (FBCA) Certificate Policy at the Basic assurance level and the Identity Vetting requirements of NIST Special Publication 800-63-1. However, this CP is also intended to specify policies that further constrain the conditions under which a Direct Trust Community conformant digital certificate may be issued, utilized and managed. In any case where this CP is found inconsistent or incompatible with the FBCA CP or NIST SP800-63-1, the incompatibilities will be addressed at the time of policy mapping between the respective policies.

The terms and provisions of this CP shall be interpreted under and governed by applicable Federal law.

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 Direct 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 Direct Trust Community X.509 Certificate Policy (DirectTrust CP) describes the unified policy under which a conforming Certificate Authority operates. Specifically, this document defines the creation and life-cycle management of X.509 version 3 public key certificates for use in applications supporting Direct Project message exchange.

1.1.1 Certificate Policy (CP)

Digital Certificates that conform to this CP may contain at minimum, one registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to a specific level of assurance established by this Certificate Policy (CP) which shall be available to Relying Parties. A certificate issued by a conforming CA may assert the appropriate OID(s) in the *certificatePolicies* extension.

1.1.2 Relationship between this DirectTrust CP and a Corresponding CPS

DirectTrust.org (“DirectTrust”) may publish a Certification Practices Statement (CPS) showing how it supports establishment of conformance to this CP. Alternatively, it may establish and document procedures to support the publishing of a Declaration of Conformance by CAs issuing digital certificates conforming to the requirements of this CP. DirectTrust may also support the establishment and utilization of an accreditation program to certify a conforming CPS and the operations and policies of its producer to the standards outlined by the accreditation program.

1.1.3 Relationship between this DirectTrust CP and the CA CP

A conforming CA may assert a mapping between its CP and this DirectTrust CP in the *policyMappings* extension of its CA certificate.

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)]

id-DTorg arc		1.3.6.1.4.1. 41179
id-DTorg-policies	id-DTorg.(0)	1.3.6.1.4.1. 41179.0
DT.org CP Versions	id-DTorg-policies.(version)	1.3.6.1.4.1. 41179.0.1
Id-DTorg-LoAs	id-DTorg.(1)	1.3.6.1.4.1. 41179.1
DT.org LoA 1	id-DTorg-LoAs.(1)	1.3.6.1.4.1. 41179.1.1
DT.org LoA 2	id-DTorg-LoAs.(2)	1.3.6.1.4.1. 41179.1.2
DT.org LoA 3	id-DTorg-LoAs.(3)	1.3.6.1.4.1. 41179.1.3
DT.org LoA 4	id-DTorg-LoAs.(4)	1.3.6.1.4.1. 41179.1.4
Id-DTorg-Cat	id-DTorg.(2)	1.3.6.1.4.1. 41179.2
DT.org CE	id-DTorg-Cat.(1)	1.3.6.1.4.1. 41179.2.1
DT.org BA	id-DTorg-Cat.(2)	1.3.6.1.4.1. 41179.2.2
DT.org HE	id-DTorg-Cat.(3)	1.3.6.1.4.1. 41179.2.3
DT.org Patient	id-DTorg-Cat.(4)	1.3.6.1.4.1. 41179.2.4

This document is version 1.2 of the DirectTrust Community X.509 Certificate Policy and is referenced by the OID 1.3.6.1.4.1. 41179.0.1.

NOTE: Prior versions of this CP exist under a different OID arc. Previous versions were associated with the "Draft for Trial Use" version of this CP and are also incorporated here for legacy and backwards compatibility. The Previous CP OID is:

joint-iso-itu-t(2) country(16) us(840) organization(1) HL7 (113883) externalUseRoots(3) DirectTrust(1313) policies(0) CP(1) i.e. 2.16.840.1.113883.3.1313.0.1

Certificates issued by a CA that are in conformance with this CP at a known level of assurance (LoA) and/or conform to the requirements for a given healthcare entity category (Cat) may assert that by listing the appropriate OID or OIDs representing the corresponding LoA as defined above in the *certificatePolicies* X.509v3 standard extension. See sections 3.2.2 and 3.2.3.1 for details of each LoA and Cat.

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 are 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 conforming CAs, each referencing a common set of policy OIDs, that the relying party may include in its set of trust anchor certificates. This will require that issuing CAs that conform to the DirectTrust profiles will need to 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 to partition LoAs. 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 the 2 trust bundles since those are the only LoAs 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

The following are roles relevant to the administration and operation of the PKI.

1.3.1 PKI Authorities

1.3.1.1 Direct Project

The Direct Project (http://wiki.directproject.org/) developed the original Direct Ecosystem Community Certificate Policy Version 0.9 in accordance with its consensus process. This DirectTrust Community Certificate Policy modifies that document so that it can be referenced in Direct Project-compliant digital certificates and to provide a set of policies under which conforming CAs may publish their related Certification Practices Statement and attest to their compliance with this CP.

1.3.1.2 DirectTrust

DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. The establishment of DirectTrust was anticipated in the Direct Ecosystem Community Certificate Policy Version 0.9 that was developed and published by the Direct Project Rules of the Road Workgroup in accordance with the Direct Project consensus process. DirectTrust operates the Direct Trust Policy Authority (DTPA) that is responsible for this CP, the approval of related practice statements, and overseeing the conformance of CA practices with this CP.

1.3.1.3 Certification Authorities (CAs)

A certification authority (CA) in this context is an entity that signs certificate signing requests (CSRs) and issues public key X.509 certificates to Direct exchange or Direct Project organizational or individual Subscribers. A CA must create a Certification Practices Statement that is conformant to the policies of this CP. For ease of reference herein, all CAs issuing certificates in accordance with this CP are hereafter referred to as “Issuer CAs”.

1.3.2 Registration Authorities (RAs)

Registration Authorities (RA) operate identity management systems (IdMs) and collect and verify Subscriber information on the Issuer CA’s behalf. RAs collect and verify identity information from Direct Subscribers using procedures that implement the identity validation policies set forth in this document. The requirements in this CP apply to all RAs. An Issuer CA shall monitor each RA’s compliance with this policy, the CPS, and if applicable, any Registration Practices Statement (RPS) under which the RA operates. An Issuer CA that relies on a variety of RAs or IdMs to support various communities of interest may submit an RPS for each RA or IdM to the DTPA for approval. The RPS must contain details necessary for the DTPA to determine how the RA achieves compliance with this Policy. Necessary details include how the RA’s process or IdM establishes the identities of applicants, how the integrity and authenticity of such identifying information is securely maintained and managed, and how changes and updates to such information are communicated to the Issuer CA. The DTPA may also utilize formal accreditation processes that Direct Trust establishes to achieve certification of RA entities.

1.3.3 Subscribers

A Direct Subscriber is an entity who uses Direct services and PKI to support Direct transactions and communications. Subscribers are not always the party identified in a certificate, such as when Direct Organizational certificates are issued to a Health Domain address. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the subject of the certificate and the entity that contracted with the Issuer CA for the certificate's issuance in accordance with this certificate policy. A Subscriber may contract a third party to manage their subscriptions, e.g. in the case of a Group certificate managed by a HISP, an authorized officer at the HISP is also a Subscriber, and each Subscriber must abide by the required Subscriber Agreements. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

1.3.3.1 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 X.509 digital certificate. Acting in the capacity of an agent for the Subscriber, the HISP may hold and manage PKI private keys associated with a Direct digital certificate on behalf of the Subscriber.

1.3.4 Relying Parties

A Relying Party uses a Subscriber's X.509 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

No stipulation.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary anticipated use for a Direct Trust Community X.509 certificate is in the exchange of electronic messages grounded in the specification of the Direct Project. This includes S/MIME message signature verification and S/MIME message encryption. Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the certificate. However, each Relying Party must evaluate the application environment and associated risks before deciding on whether to accept a certificate issued under this CP for a particular transaction.

1.4.2 Prohibited Certificate Uses

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

DirectTrust through the Direct Trust Policy Authority (DTPA) or such other entity as it may designate is responsible for managing and facilitating a consensus process for approval and administration of this document that is aligned with the practices and procedures of the Direct Project.

1.5.2 Contact Person

Questions regarding this certificate policy should be directed to:
DirectTrust, Inc.
Phone: 202-862-0619
E-mail: kibbedavid@mac.com, or Admin-CP@DirectTrust.org
Mail: 1101 Connecticut Avenue NW, Suite 1000 Washington, DC 20036

Web: http://www.directtrust.org/

1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

The Certification Practices Statement states how the CA establishes the assurance required by the corresponding Certificate Policy of the CA. Each CA is responsible for asserting that the CPS conforms to their CP and that their CP maps to the requirements of this DirectTrust CP.
The CA must designate the person or organization authorized to make these assertions.

The DirectTrust may operate an accreditation program that certifies the compliance of Issuing CA CPSs to this CP. In each case, DirectTrust will be solely responsible for making the determination of suitability; however, DirectTrust's determination may be based on any available compliance auditor's results and recommendations. See Section 8 for further details.

1.5.4 Certification Practices Statement Approval Procedures

Each conforming CA shall submit the related CPS to a compliance analysis and audit against this CP as described in Section 8 of this CP. The CA's CPS shall be required to meet all facets of its policy. The CA may not declare conformance with this CP until the compliance analysis and audit is complete and all discrepancies resolved. DirectTrust may operate an accreditation program that may certify the compliance analysis and audit results.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Acronym	**Meaning**
CA	Certification Authority
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DN	Distinguished Name
DTPA	Direct Trust Policy Authority
ID	Identity
IETF	Internet Engineering Task Force
ISSO	Information Systems Security Officer
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

1.6.2 Definitions

Term	**Definition**
Certificate	A digital representation of information which 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	An authority trusted by one or more users to create and assign certificates. Also known as a Certificate Authority.
Certificate Policy	A Certificate Policy 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.
Certificate Practice Statement	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements typically provided in a certificate policy.
Certificate Revocation List	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Direct Project	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.
Internet Engineering Task Force	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
Information Systems Security	An individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to Information

Officer (ISSO)

Systems Security, to ensure information assets are adequately protected.

Private Key

(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.

Public Key

(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.

Public Key Infrastructure

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

Entity responsible for identification and authentication of certificate subjects.

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.

Subscriber

A Subscriber is an entity that does not itself issue certificates to another party and is either (1) the subject named or identified in a certificate issued to that entity, or (2) holds, directly or through its designated HISP (or other authorized third party), a private key that corresponds to the public key listed in the certificate.

2 Publication and Repository Responsibilities

2.1 Repositories

Conforming CAs and RAs shall operate repositories in support of operations required by this CP and related CPS. At a minimum, an Issuing 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 conforming Issuing CA should maintain a Certificate Revocation List (CRL) and expose its location in the CRL Distribution Points X.509v3 extension. A conforming CA may also choose to maintain an equivalent Online Certificate Status Protocol (OCSP) Responder and expose its location in the Authority Information Access X.509 extension. If a CA maintains an OCSP Responder, it must do so in accordance with the relevant Sections within 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 Issuing CA must publish its CA certificate and any other intermediate or trust anchor certificates necessary to validate the Issuing CA.

2.2.2 Publication of CA Information

Each conforming CA shall publish information concerning the CA necessary to support its operation and use. Information on how to obtain a copy of this certificate policy shall be provided to any party with legitimate interest. Issuing 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 certificate policy, and any ensuing changes, shall be made available within 14 days of approval through the DirectTrust consensus process. CRLs from conforming CAs must expire every 30 days or less and must be updated immediately when a new entry is added to it, or every 30 days, whichever is earlier.

2.4 Access Controls on Repositories

Conforming CAs and RAs shall protect repository information not intended for public dissemination or modification. Conforming 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. As specified in the Direct Project Applicability Statement for Secure Health Transport, certificates tied to full Direct addresses ("Address certificates") shall contain the Direct address in the *subjectAltName* extended attribute as an rfc822Name. Certificates tied to a Direct domain ("Organizational certificates") shall contain the domain name in two places:

1. The *subjectAltName* extension formatted as a dNSName, and
2. The CN of the Subject DN.

3.1.2 Need for Names to be Meaningful

Names used in certificates shall uniquely identify the organization or person to which they are assigned 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

Conforming 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 may 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 RA, no proof of private key possession is required. In the case where the Subscriber named in the certificate 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 conforming CA. The conforming 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 organizational certificates must include the organization name, mailing address, and documentation of the existence of the organization as well as the requested domain name that will appear in the certificate (see section 3.1.1 for details).

The requesting organization must be qualified in one of the following categories:

- HIPAA Covered Entity.
- HIPAA Business Associate, or
- Healthcare-related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. Each organizational certificate must represent a legally distinct entity.

Accordingly, the Issuer CA or the RA shall verify the applicant organization’s healthcare category in accordance with the process established in its CPS or RPS that meets the following minimum requirements:

DT.org CE	Applicant represents that it is a Covered Entity as defined in HIPAA.
DT.org BA	Applicant represents that it will limit its use of any Digital Certificate issued to it pursuant to this CP for purposes required in its capacity as a Business Associate (BA), as defined in HIPAA. The RA will confirm that such representation has been made in an appropriate legally binding agreement.. Relying Parties may be required by government statute or regulations to have additional agreements in place with the BA.

DT.org HE	Applicant represents that it will limit its use of any Digital Certificate issued to it pursuant to this CP for purposes required in its capacity as a Non-HIPAA Healthcare Entity (HE), defined as an entity that has an appropriate healthcare-related need to exchange Direct messages and which agrees to handle protected health information with privacy and security protections that are equivalent to those required by HIPAA. The RA will confirm that such representation has been made in an appropriate legally binding agreement. For each HE, Relying Parties are responsible for determining if Direct message exchange is appropriate.

The RA shall verify the organization information submitted, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

If a certificate asserts an organizational affiliation between a human Subscriber and an organization (e.g. Direct Organizational Certificates), the conforming CA shall obtain documentation from the organization that recognizes the affiliation and obligates the organization to provide updates on Subscribers' access to Group certificates where applicable or to request modification or revocation of the certificate where necessary, if that affiliation ends. See Sections 3.2.3.3, 3.2.5, 4.9.1 and 9.6.1.

Note: Certificates asserting an organizational affiliation may also assert the OID corresponding to that organization's healthcare category.

3.2.3 Authentication of Individual Identity

3.2.3.1 Authentication of Human Subscribers

Validation of the identity of an individual is required in several cases: (1) To verify the identity of a representative of an organization requesting a DirectTrust Organizational certificate; (2) To verify the identity of an Information Systems Security Officer (ISSO) (or equivalent) at the organization physically controlling the private key in the case of a Group certificate; (3) To verify the sponsor of a Device certificate; and (4) To verify the identity of an individual requesting a DirectTrust Address certificate.

The Issuer CA or the RA shall verify an individual's identity in accordance with the process established in its CPS or RPS that meets one of the following requirements and shall designate which LoA was followed:

DT.org LoA 1	Applicant's control over an email address (or any of the identity verification methods listed for a higher level).

(Equivalent to NIST 800-63-1 Level 1 or Kantara Level 1 or FBCA Rudimentary)	
DT.org LoA 2 (Equivalent to NIST 800-63-1 Level 2 or Kantara Level 2 or FBCA Basic)	Applicant supplies his or her full legal name, an address of record, and date of birth. For **In-Person vetting**: the applicant also provides valid government issued photoID. **RA** inspects photo-ID; compares picture to Applicant; and records the ID number, address and date of birth (DoB) **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 claimed address after issuance. For **Remote vetting**: the applicant provides valid government issued PhotoID identifier + a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID or account. **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, when applicable). **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 verification methods listed for a higher level are also acceptable.

DT.org LoA 3 (Equivalent to NIST 800-63-1 Level 3 or Kantara Level 3 or FBCA Basic or Medium)	Applicant supplies his or her full legal name, an address of record, and date of birth. For **In-Person vetting**: the applicant also provides valid government issued photoID. **RA** inspects 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. **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 claimed address after issuance. For **Remote vetting**: the applicant provides valid government issued PhotoID identifier + a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID and account. **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, when applicable). **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 a physical address associated with the Applicant in the records. If the telephone method is used, CA also records Applicant's voice or uses alternative means that establish an equivalent level of non-repudiation. Any of the identity verification methods listed for a higher level are also acceptable.

DT.org LoA 4 (Equivalent to NIST 800-63-1 Level 4 or Kantara Level 4 or FBCA Medium)	Applicant supplies his or her full legal name, an address of record, and date of birth. For **In-Person vetting**: the applicant also provides valid government issued photoID + a second independent government ID or financial account. **RA** inspects photo-ID; compares picture to Applicant; and verifies both IDs and/or 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. A current biometric (e.g. photo or fingerprints) is recorded. **CA** issues credentials in a manner that confirms the address associated with the Applicant in the records.

If the requested Direct digital certificate is to be used by a patient or on behalf of a patient, the Issuer CA or the RA shall verify the patient identity with the process established in its CPS or RPS that meets any of the above LoA requirements and collects the following Subscriber representation, and shall designate which LoA was followed:

DT.org Patient	Applicant represents that any Digital Certificate issued pursuant to this CP will be used for their personal healthcare Direct message exchange purposes. The RA verifies that the patient or the patient's authorized representative has made this representation.

3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

No stipulation.

3.2.3.3 Authentication of Human Subscribers for Group Certificates

A Group certificate corresponds to a credential with a private key that is shared by multiple Subscribers. A DirectTrust certificate that is held and managed by a Health Information Service Provider (HISP) on behalf of a Subscriber organization is an example of a group certificate. Identity Verification of the Subscriber organization and its representative is covered in sections 3.2.2 and

3.2.3.1.

For HISP managed group certificates, a conforming CA and/or RAs shall also record the information identified in Section 3.2.3.1 for the Information Systems Security Officer (or equivalent) of the HISP, 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 HISP Information Systems Security Officer or equivalent shall be responsible for ensuring control of the private key, including maintaining a list of any Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time.
- The subjectName DN 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 list of those holding the shared private key must be provided to, and retained by, the applicable CA or its designated representative.

3.2.3.4 Authentication of Devices

An Issuer CA may issue a certificate for use on a computing or network device. In such cases, the device must have a human sponsor who provides:

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

Registration shall also include verification of the sponsor 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).
- 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 certificate's sponsor changes, the new sponsor shall review the status of each device to ensure it is still authorized to receive certificates. The CPS of a conforming CA shall describe procedures to ensure that certificate accountability is maintained.

3.2.4 Non-verified Subscriber Information

All Subscriber information placed in a Direct Trust certificate must be verified and a certificate issued within 30 days of completion of verification.

3.2.5 Validation of Authority

The conforming RA must verify the association between an organization requesting an organizational certificate and the individual representing the organization.

3.2.6 Criteria for Interoperation

To be deemed a conforming Direct Trust Issuing CA, the CA shall issue certificates according to this certificate policy or by a certificate policy that meets equivalent criteria.

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 Direct Trust certificate must be established through the initial identity verification 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 Direct Trust certificate is revoked, the Subscriber shall go through the initial identity verification 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 Direct Trust X.509 certificate.

4.1.1 Submission of Certificate Application

A Direct Trust HISP or Subscriber creates the official certificate signing request based on input received from the Subscriber as validated by the RA or CA during the identity verification process.

4.1.2 Enrollment Process and Responsibilities

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

4.2 Certificate Application Processing

The conforming Direct Trust CA and RA are responsible for verifying that the information in a certificate signing request is accurate and reflect the information presented by the Subscriber.

4.2.1 Performing Identification and Authentication Functions

The identity verification of Subscribers shall be done by the conforming Direct Trust CA or RA as specified in section 3.2 using procedures detailed in the applicable conforming CPS or RPS.

4.2.2 Approval or Rejection of Certificate Applications

A certificate application may be rejected by a conforming Direct Trust CA due to missing or inaccurate information. Each conforming Direct Trust CA governing body retains the right to reject Direct Trust certificate applications if, in its judgment, the requesting individual or organization does not have a legitimate reason to possess a Direct Trust certificate.

4.2.3 Time to Process Certification Applications

All Subscriber information placed in a Direct Trust certificate must be verified and a certificate issued within 30 days of completion of verification.

4.3 Issuance

4.3.1 CA Actions During Certificate Issuance

The conforming Direct Trust CA will ensure that the public key is bound to the correct Subscriber and generate the X.509 certificate. The conforming Direct Trust CA will publish the certificate as specified in section 4.4.2. The Issuer CA shall perform its actions during the certificate issuance process in a secure manner.

4.3.2 Notification to Subscriber of Certificate Issuance

The Subscriber must be notified via physical mail or email that his certificate has been issued.

4.4 Certificate Acceptance

4.4.1 Conduct Constituting Certificate Acceptance

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

4.4.2 Publication of the Certificate by the CA

The appropriate entity may publish Subscriber certificates in a directory specified in section 2.2.1. An Issuing CA is required to publish its CA certificate to the repository.

4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

4.5 Key Pair and Certificate Usage

4.5.1 Subscriber Private Key and Certificate Usage

Subscribers or their authorized HISP representatives, who take possession of their private key, shall protect it from access by unauthorized parties and shall use their Private Keys only as specified in the key usage extension of the corresponding Certificate.

4.5.2 Relying Party Public Key and Certificate Usage

Direct Trust certificates shall conform to the policies provided by this certificate policy. Relying parties should understand these policies. The conforming Direct Trust CA must publish a certificate revocation list (CRL) 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. Reducing the validity period of Subscriber certificates may assist in reducing the size of CRLs. 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 conforming Direct Trust CA re-keys.

4.6.2 Who May Request Renewal

The conforming Direct Trust CA may request renewal of its own certificate. For Subscriber certificates, the Subscriber himself or their authorized representative, or the conforming Direct Trust RA may request renewal.

4.6.3 Processing Certificate Renewal Requests

The conforming Direct Trust CA shall approve or reject Subscriber certificate renewal requests. Identity verification of the Subscriber shall be equivalent to the initial identity verification process or executed via proof of possession of the private key through a digital signature.

4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

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

4.6.6 Publication of the Renewal Certificate by the CA

The conforming Direct Trust CA 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 distributionPoint 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

A conforming Direct Trust RA or the Subscriber or their authorized representative may request the re-key of a Subscriber certificate.

4.7.3 Processing Certificate Re-Keying Requests

The conforming Direct Trust CA shall approve or reject Subscriber certificate re-keying requests. Identity verification of the Subscriber shall be equivalent to the initial identity verification.

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 may or may not be revoked, but must not be further re-keyed, renewed, or modified.

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 conforming Direct Trust RA may request modification of a Subscriber certificate.

4.8.3 Processing Certificate Modification Requests

Identity verification for a certificate modification request shall be accomplished using one of the following processes:

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

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 are:

- identifying information or affiliation components of any names in the certificate become invalid,
- the Subscriber can be shown to have violated the stipulations of its Subscriber agreement,
- the private key is suspected of compromise, and the Subscriber asks for his/her certificate to be revoked.

Whenever any of the above circumstances occur, the associated certificate shall be revoked and placed on the certificate revocation list (CRL) and, when applicable, have its revoked status reflected in OCSP responses.

4.9.2 Who Can Request Revocation

The CA/RA may request revocation of a certificate, or the issuing CA may entertain requests from a Subscriber or their authorized representative to revoke a certificate.

4.9.3 Procedure for Revocation Request

Any request for certificate revocation shall identify the certificate to be revoked by serial number and explain the reason for revocation. A conforming Direct Trust RA and CA 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, the conforming Direct Trust CA will place the certificate's serial number and any other required information on its certificate revocation list (CRL) and/or 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 authorized PKI entities 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

A conforming Direct Trust 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

The matter of how often new revocation data should be obtained is a determination to be made by the

Relying Party.

4.9.7 CRL Issuance Frequency

A Direct Trust CRL must be issued and posted to the repository listed in section 2.2.1 every 30 days when there are no changes or updates to be made to ensure timeliness of information. A CRL may be issued more frequently than every 30 days if new entries are made to the CRL. The conforming Direct Trust 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 upon generation but within no more than four hours after generation. Furthermore, a new CRL shall be published no later than the time specified in the nextUpdate 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

No stipulation.

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. Direct Trust 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

Direct Trust 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

Direct Trust 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 the 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,
- 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,
- 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
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with its Certification Practice Statement (CPS).

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

The CA governance entity shall take appropriate administrative and disciplinary actions against personnel 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 Issuing 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, where appropriate
- The identity of the entity and/or operator (of the Issuing CA) that caused the event,

Detailed audit requirements are listed in the table below. All security auditing capabilities of the Issuing 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

Auditable Event
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

Auditable Event
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

Auditable Event
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)

Auditable Event
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

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:

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

5.5.2 Retention Period for Archive

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 CA will 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 private signing 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.

The CA self-signed root certificate shall be valid for no more than 20 years.

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 a CA becomes known, it shall be investigated 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

The CA 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 the 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 private and public keys. 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.

6.1.1.2 Subscriber Key Pair Generation

The CA cryptographic keying material generated for Subscriber certificates shall be created on physical hardware that is well protected.

6.1.2 Private Key Delivery to Subscriber

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

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 1 (SHA-1)
- 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)

All but the first listed above may be utilized for Subscriber keys.

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, except for certificates issued to smart cards or other hardware devices that are incapable of accepting 2048-bit RSA certificates, then at least 1024-bit public keys for RSA, so long as such certificates expire on or before December 31, 2013.

The Issuer CA may require higher bit keys in its sole discretion.

6.1.6 Public Key Parameters Generation and Quality Checking

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

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

Direct Trust Subscriber public keys that are bound into certificates shall be certified for use in signing and encryption of S/MIME packages as required by the Direct Project specifications. Specifically, Subscriber certificates shall assert the following key usage bits:

- digitalSignature
- keyEncipherment

Subscriber certificates that are dual-use certificates MUST not assert the non-repudiation bit.

Subscriber certificates shall also assert an extended key usage bit of *emailProtection* and a BasicConstraint of *CA:FALSE*.

A conforming Direct Trust CA root certificate shall assert the following key usage bits:

- cRLSign
- keyCertSign

The CA root certificate shall also 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 shall be recommended to be minimally validated to the FIPS 140 level identified below for the relevant party (or an equivalent protection):

CA	Level 2
RA	Level 1

HISP	Level 2
Subscriber	Level 1

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

No Stipulation.

6.2.3 Private Key Escrow

Private keys (CA or Subscriber) shall not be escrowed.

Subscriber

6.2.4 Private Key Backup

The CA root private signature key shall be backed up to a secure offsite location to facilitate disaster recovery.

Subscriber private keys shall 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

No stipulation.

6.2.7 Private Key Storage on Cryptographic Module

No stipulation.

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.

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 signature keys when they are no longer needed.

Subscriber private signature keys shall be destroyed when they are no longer needed, or when the certificates to which they correspond expire or are revoked.

6.2.11 Cryptographic Module Rating

See Section 6.2.1.

6.3 Other Aspects of Key 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

A CA root private key shall be used for a maximum of 20 years. A CA root certificate shall expire after a maximum of 20 years. Subscriber private keys shall be used for a maximum of 6 years. Subscriber public certificates shall expire after one year.

6.4 Activation Data

6.4.1 Activation Data Generation and Installation

The Issuer CA or Subscriber shall generate activation data that has sufficient strength to protect its respective Private Keys. If the Issuer CA 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 CA or Subscriber may only transmit activation data via an appropriately protected channel and at a time and place that is distinct from the delivery of the associated cryptographic module.

6.4.2 Activation Data Protection

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

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

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

6.4.3 Other Aspects of Activation Data

No stipulation.

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 a trusted role and its CA system.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life-Cycle Security Controls

6.6.1 System Development Controls

CA software shall be developed in a controlled development environment with modern source code control. CA hardware and software shall be dedicated to performing the CA tasks. 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 a 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 CA system.

6.6.3 Life Cycle Security Ratings

No stipulation.

6.7 Network Security Controls

Information to be transferred from the 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 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

7.1.1 Version Numbers

Conforming Direct Trust CAs shall issue X.509 v3 certificates, which means the version field should 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 certificate policy. The CRL Distribution Points extension may be populated with a CRL URL as specified in section 2.2.1of this certificate policy. The Authority Information Access extension may be populated with an OCSP Responder location as specified in section 2.2.1 of this certificate policy. The Subject Alternative Name extension shall be populated as specified in section 3.1.1 of this certificate policy. The Certificate Policies extension shall be populated as defined in section 7.1.6 of this certificate policy.

7.1.3 Algorithm Object Identifiers

End Entity Certificates signed by a conforming Direct Trust 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}

Certificates issued by a conforming Direct Trust 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

Certificates shall assert at least one of the policy OIDs (or a policy OID of a superior CP that has been successfully mapped to this CP), defined in section 1.2 of this certificate policy.

7.1.7 Usage of Policy Constraints Extension

No stipulation.

7.1.8 Policy Qualifiers Syntax and Semantics

No Stipulation

Subscriber7.1.9 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

7.2.1 Version Numbers

A conforming Direct Trust CA shall issue X.509 version 2 CRLs, which means the version field should contain the integer 1.

7.2.2 CRL and CRL Entry Extensions

A conforming Direct Trust CA shall conform to the CRL and CRL Extensions profile defined in IETF RFC 5280.

A Direct Trust 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

A conforming Direct Trust CA may deploy an OCSP responder. No stipulation is made beyond this assertion.

8 Compliance Audits and Other Assessments

CAs and RAs shall have a compliance audit mechanism in place to ensure that the requirements of their CP/CPS 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 recommended template for a conforming CA to make a self-attested, legally binding Declaration of Conformance to this CP or a CA CP mapped to this CP and the related CPSCPS. DirectTrust may provide an accreditation program to certify the compliance of CAs, RAs, and HISPs, that includes the aforementioned attestation, that the various entities will be audited against.

8.1 Frequency and Circumstances of Assessment

The audit occurs at least every two years. DirectTrust may provide an accreditation program to certify the compliance of CAs, RAs, and 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 HISPs, in which case the program will outline the requirements in respect to identity and qualifications of assessors.

8.3 Assessor’s Relationship to Assessed Entity

The CA Declaration of Conformance shall describe the compliance assessor’s relationship to the CA, indicating whether the assessor is internal to the CA or an independent compliance auditor. DirectTrust may provide an accreditation program to certify the compliance of CAs, RAs, and 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 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 conformance 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 conformance. 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 conformance 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 Conformance or to reference a location where the Declaration of Conformance 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

A Direct Trust CA shall store private information securely.

9.4.5 Notice and Consent to Use Private Information

A Direct Trust CA shall use private information as dictated by the agreements with its Subscribers.

9.4.6 Disclosure Pursuant to Judicial/Administrative Process

A Direct Trust 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 Direct Trust 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 Issuing CA that the Subscriber will:

1. Protect its Private Keys from compromise (including if employing a HISP who uses secure processes against potential compromise),
2. Provide accurate and complete information and communication to the Issuer CA and RA,
3. Confirm the accuracy of certificate data prior to using the certificate,
4. Promptly 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,
5. 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
6. 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 Direct Trust 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 certificate policy becomes effective when approved through the DirectTrust consensus process. This certificate policy has no specified term.

9.10.2 Termination

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

9.10.3 Effect of Termination and Survival

The requirements of this certificate policy 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 certificate policy may be amended through the DirectTrust consensus process.

9.12.2 Notification Mechanism and Period

No stipulation.

9.12.3 Circumstances Under Which OID Must be Changed

No stipulation.

9.13 Dispute Resolution Provisions

In the event of any dispute related to this certificate policy, a statement of guidance may be issued and published on the DirectTrust website if approved through the DirectTrust consensus process.

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

Should it be determined that one section of this certificate policy is incorrect or invalid, the other sections of this certificate policy shall remain in effect until the certificate policy is updated.

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other Provisions

No stipulation.