
# Updox Direct
# Certificate & Registration Practice Statement

Version 1.4

Updated: October 30, 2019

Updox
6555 Longshore Street
Suite 200
Dublin, OH 43017
1-614-798-8170
http://updox.com

# CONTENTS

# 1 INTRODUCTION

Secure electronic message exchange is a foundational element of nationwide interoperability for the healthcare industry. Two key components of success were the adoption of 1) technical standards and 2) governance policies and practices.

*Technical Standards*
To establish the technical standards, the Office of the National Coordinator (ONC) sponsored the Direct Project initiative which created the Direct Project Applicability Statement for Secure Health Transport specification. The specification allows participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. It is based on S/MIME message signatures and message encryption for the purposes of achieving privacy, authentication, message integrity, and non-repudiation.

There are three main roles in the Security and Trust Framework that support Direct exchange:

- Registration Authority (RA) – verifies identity for a Certificate Authority
- Certificate Authority (CA) – issues/manages certificates based on input from an RA
- Health Information Services Provider (HISP) – encrypts/decrypts and transports Direct messages

*Governance Policies*
To establish the governance policies, DirectTrust was formed. DirectTrust is a non-profit, competitively neutral, self-regulatory entity created by and for Direct community participants. The goal is to develop, promote and, as necessary, help enforce the rules and best practices necessary to maintain security and trust within the Direct community, and to foster widespread public confidence in the Direct exchange of health information. The DirectTrust governance policies are:

- Certificate Policy (CP)
- HISP Policy (HP)

DirectTrust Certificate Policy – describes the policy requirements that pertain to the Registration Authority and the Certificate Authority. This policy was based upon:

- Internet Engineering Task Force (IETF) - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647)
- Federal Bridge Certificate Authority (FBCA) – Certificate Policy (basic assurance)
- National Institute of Standards (NIST) – Identity Verification (SP 800-63-2)

DirectTrust HISP Policy – describes the policy requirements for the Health Information Services Provider.

*Governance Practice Statements*
Conforming RA, CA, and HISP vendors publish practice statements that describe their policies/practices that correspond to the DirectTrust policies. The vendor specific practice statements are:

- Registration Practice Statement (RPS)
- Certificate Practice Statement (CPS)
- HISP Practice Statement (HPS)

When a vendor is both the RA and CA, the practice statements may be combined in a single document.

## 1.1 Overview

Updox serves as the Registration Authority, Certificate Authority, and Health Information Services Provider for its Direct exchange service.

This document is the Updox Certificate and Registration Practice Statement (referred to as the CPS). It describes the policies and practices for the creation and life-cycle management of X.509 version 3 public key certificates as well as identity verification.

The Updox HISP Practice Statement is a separate document.

This document is compliant with the Direct Project Applicability Statement for Secure Health Transport specification.

### 1.1.1 Certification Policy

This CPS is based on the DirectTrust Certificate Policy (CP) version 1.4.

Updox digital certificates contain three registered policy object identifiers (OIDs), which a Relying Party may use to decide whether a certificate is trusted for a particular purpose. These OIDs specify the DirectTrust CP version, the identity proofing Level of Assurance, and the Healthcare Category for the Subscriber. The OIDs are located in the *certificatePolicies* extension of the Updox certificates.

### 1.1.2 Relationship between the DirectTrust CP and Updox CPS

This document describes how Updox supports compliance with the DirectTrust CP.

### 1.1.3 Relationship between the DirectTrust CP and Updox CA CP

The Updox CA certificate specifies the mapping between the DirectTrust CP and the Updox CPS in the *policyMappings* extension.

### 1.1.4 Relationship between the DirectTrust CP and DirectTrust-EHNAC Accredited Entities

Updox is compliant with the DirectTrust CP 1.4 and accredited by:

- DirectTrust – HISP program
- EHNAC – HISP Privacy & Security, RA, and CA

## 1.2 Document Name and Identification

This document is the Updox Direct Certificate Practice Statement (CPS).

The Updox certificates contain the following object identifiers (OIDs) that identify the DirectTrust Certificate Policy version, the identity verification level of assurance, and the healthcare category:

- DirectTrust CP 1.3.6.1.4.1.41179.0.1.4
- DirectTrust Identity LoA 1.3.6.1.4.1.41179.1.3
- Healthcare Category
  - Covered Entity 1.3.6.1.4.1.41179.2.1
  - Business Associate 1.3.6.1.4.1.41179.2.2
  - Healthcare Entity 1.3.6.1.4.1.41179.2.3
  - Patient 1.3.6.1.4.1.41179.2.4
  - Non-Declared 1.3.6.1.4.1.41179.2.5

## 1.3 PUBLIC KEY INFRASTRUCTURE (PKI) PARTICIPANTS

### 1.3.1 Certificate 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 the DirectTrust CP.

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. Updox operates under this Certification Practices Statement (CPS) that is reviewed as part of the accreditation process to ensure compliance to the policies of the DirectTrust CP.

Updox performs the role of CA.

### 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 the DirectTrust CP apply to all RAs. An Issuer CA will monitor each RA's compliance with this policy, the CPS, and if applicable, any Registration Practices Statement (RPS) under which the RA operates. 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.

Updox performs the role of RA. The registration practices are documented in this CPS instead of a separate RPS.

#### 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.

### 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. A Direct Subscriber is an entity who uses Direct services and PKI to support Direct message exchange. Prior to proofing of identity and issuance of a certificate, a Subscriber is an Applicant.

#### 1.3.3.1 Custodian

A Custodian acts in the capacity of an agent for the Subscriber for the purposes of enabling health information exchange by holding and managing Private Keys associated with a Certificate on behalf of that Subscriber in a Custodial Subscriber Key Store.

#### 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 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. Updox performs the role of HISP.

#### 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 Party (RP)

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

#### *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).

Patients are Subscribers. An individual granted proxy account access by a patient, such as a parent of a minor, spouse or health care proxy for an elderly person, is considered an Affiliate.

### 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 CPS

Updox is responsible for managing and facilitating a consensus process for approval and administration of this document to ensure alignment with the DirectTrust certificate policy.

### 1.5.2 Contact Person

Questions regarding this certificate practice statement (CPS) should be sent to:

Updox
Attn: Compliance Director
6555 Longshore Street, Suite 200
Dublin, OH 43017 USA
1-614-798-8170 x126
directadmin@updox.com

### 1.5.3 Person Determining CPS Suitability for the Policy

The Updox management team ensures this CPS is compliant with the DirectTrust certificate policy.

## 1.6 DEFINITIONS AND ACRONYMS

### 1.6.1 Acronyms

| Acronym | Meaning |
|---|---|
| BAA | Business Associate Agreement |
| CA | Certification Authority |
| CE | Covered Entity |
| CFR | Code of Federal Regulations |
| CP | Certificate Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| DC | Data Center |
| DN | Distinguished Name |
| DNS | Domain Name System |
| DTPC | DirectTrust Policy Committee |
| EHNAC | Electronic Healthcare Network Accreditation Commission |

| Acronym | Meaning |
|---|---|
| HE | Healthcare Entity |
| HIPAA | Health Insurance Portability and Accountability Act |
| HISP | Health Information Services Provider |
| HSM | Hardware Security Module |
| ID | Identity Document |
| IdM | Identity Management |
| IETF | Internet Engineering Task Force |
| ISSO | Information Systems Security Officer |
| LoA | Level of Assurance |
| NIST | National Institute of Standards Technology |
| 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 |
| SHA | Secure Hash Algorithm |
| S/MIME | Secure Multipurpose Internet Mail Extensions |
| TA | Trusted Agent |

### 1.6.2 Definitions

| Term | Definition |
|---|---|
| Address-Bound Certificate | An Address-Bound Certificate is a Certificate that contains a full Direct Address in the form of an RFC822 email address in the Certificate *subjectAlternativeName* 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. |

| Term | Definition |
|---|---|
| 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 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. |
| Certificate 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 (CP) | 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. |
| Certificate Practice Statement (CPS) | 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 (CRL) | 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. |
| 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. |
| Custodian | A Custodian is an organization that operates a Custodial Subscriber Key Store. |

| Term | Definition |
|---|---|
| Device | A Device is a non-human Subscriber of a Certificate. Examples of Devices include but are not limited to routers, firewalls, servers, imaging systems, consumer diagnostics, cameras, and other devices capable of securely handling Private Keys and properly implementing PKI technologies, either directly or through a 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 together with the "@" symbol. Examples: johndoe@direct.sunnyfamilypractice.example.org, er@direct.hospital.org |
| 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. |
| 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 |
| Domain Name System (DNS) | The Domain Name System (DNS) is a hierarchical naming system built on a distributed database for computers, services, or any resource connected to the Internet or a private network. |
| 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). |

| Term | Definition |
|---|---|
| Health Information Service Provider (HISP) | A separate business organization that provides the management of security and transport as it relates to information exchange using Direct Project standards on behalf of the sending or receiving organization or individual. For purposes of this CPS, the HISP is Updox. |
| HIPAA | The Health Insurance Portability and Accountability Act of 1996, as amended. |
| HIPAA Representative | A HIPAA Representative is a person named by a patient granting authority to have access to the Patient's protected health information. A HIPAA Representative does not have authority to make health care decisions for the Patient. |
| Internet Engineering Task Force (IETF) | The Internet Engineering Task Force (IETF) is a standards development organization responsible for the creation and maintenance of many Internet related technical standards. |
| Information Systems Security Officer (ISSO) | The Information System Security Officer (ISSO) is an individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to information systems security, to ensure information assets are adequately protected. |
| Issuer or Issuing CA | An Issuer CA is a CA issuing Certificates in conformance with this CP. |
| 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 LoAs as defined in NIST SP 800-63. |
| National Provider Identifier (NPI) | 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. |
| Object Identifier (OID) | A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. |

| Term | Definition |
|---|---|
| Online Certificate Status Protocol | An internet protocol used for obtaining Certificate Revocation Lists. |
| 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 is an Address Certificate issued to a Patient containing a full Direct Address in the form of an RFC822 email address in the Certificate *subjectAlternativeName* extension. |
| 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 | 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 (PKI) | 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 (RA) | 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. |

| Term | Definition |
|---|---|
| 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. |
| Updox Data Center | The SOC1 (SSAE 16) and SOC2 Type 2 audited data center that hosts the certificate infrastructure. The data center is compliant with HIPAA, PCI-DSS, IRS 1075 and Tier IV data center standards, and backed by 24×7 on-site security. |
| Updox Direct | Updox-owned and operated HISP which provides the management of security and transport as it relates to information exchange using Direct Project standards. |
| Updox Direct Administrator | The person who is tasked with responsibility for distribution and use of Updox Direct capabilities within their respective organization. |
| User | A User is an individual authorized by a Subscriber to access or make use of a Private Key corresponding to a Certificate for the purpose of originating or accepting delivery of Direct messages. |

# 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 REPOSITORIES

The Updox repositories that support all RA, CA, and HISP operations are located at its 3rd party data center. These repositories contain the CP/CPS, RP Agreements, Subscriber Agreements, CA certificates and validation chains, End Entity certificates, CRLs, and CSS data. Remote access by authorized personnel is via a Virtual Private Network (VPN). Frequency of publication is in real time.

### 2.1.1 Repository Obligations

The Updox certificate repository is available 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

The Certificates are hosted in the Updox DNS and discoverable via the URL in the Common Name field of the end entity certificate.

Updox maintains a Certificate Revocation List (CRL) and exposes its location in the CRL Distribution Points X.509v3 extension. The certificate revocation list (CRL) is available at: http://updoxdirect.com/pki/CRL1.4.crl.

Updox certificates only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties. Updox publishes its CA certificate and any other intermediate or trust anchor certificates necessary to validate the Issuing CA.

### 2.2.2 Publication of CA Information

Updox publishes this CPS at: http://updoxdirect.com/pki/CPS1.4.pdf.

### 2.2.3 Interoperability

No stipulation.

## 2.3 FREQUENCY OF PUBLICATION

The CPS is published within 14 days of approval through the Updox consensus process.

The CRL is published every 18 hours regardless if changes occur or not.

## 2.4 ACCESS CONTROLS ON REPOSITORIES

Updox protects repository information not intended for public dissemination or modification.

Updox provides unrestricted read-only access to its repositories for legitimate uses. Unauthorized persons are prevented from creating, deleting, or modifying entries in the repositories through logical and physical security measures.

# 3 IDENTIFICATION AND AUTHENTICATION

## 3.1 NAMING

### 3.1.1 Types of Names

Updox certificates use non-null Distinguished Name (DN) forms for the issuer and subject names.

Address-Bound certificates contain a full Direct Address in the form of a rfc822Name in the *subjectAlternativeName* extension of the certificate.

Domain-Bound Certificates contains a Health Domain Name in the form of a dNSName in the subjectCommonName and subjectAlternativeName extensions of the Certificate.

The Updox CA certificate DN attributes are:

| Attribute | Value |
|---|---|
| Country (C) = | US |
| Organization (O) = | Updox LLC |
| Organizational Unit (OU) = | Not used |
| State or Province (S) = | Not used |
| Locality (L) = | Not used |
| Common Name (CN) = | Updox Accredited Direct CA1.4 |

The Updox end entity DN attributes are:

| Attribute | Value |
|---|---|
| Country (C) = | US |
| Organization (O) = | Domain Cert – Subscriber Organization Name Address Cert – Updox LLC |
| Organizational Unit (OU) = | Not used |
| State or Province (S) = | Not used |
| Locality (L) = | Not used |
| Common Name (CN) = | Subscriber Organization Direct Email Domain Name |
| E-Mail Address (E) = | Not used – Info is in subjectAltName extension |

### 3.1.2 Need for Names to be Meaningful

Names used in certificates uniquely identify the organization or person to which they are assigned and can be easily understood by humans.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

Updox does 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

Updox enforces name uniqueness of the certificate subject DN within the Updox 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. Updox may reject any application or require revocation of any certificate that is part of a trademark dispute.

## 3.2 INITIAL IDENTITY VALIDATION

Updox is the Registration Authority for its own Direct messaging CA and HISP services. Updox issues both domain-bound and address-bound certificates.

### 3.2.1 Method to Prove Possession of Private Key

Updox generates the Private Key on behalf of the Subscriber; therefore, no proof of Private Key possession is required.

### 3.2.2 Authentication of Organization Identity

For certificates that assert an organization affiliation, Updox requires:

- Organization name and mailing address
- Documentation of the legal existence of the organization
- Health domain/endpoint name
- Organization to have the right to use the health domain name
- Organization to be a legally distinct entity
- Healthcare category (as defined by HIPAA at 45 CFR 160.103) and attestation
    - Covered Entity
    - Business Associate
    - Healthcare Entity

In the certificate the:

- Organization will be specified in the (O) field of the *subjectDistinguishedName*
- Healthcare category OID will be specified as a *certificatePolicy*

If a certificate asserts an organization affiliation, the organization must:

- Maintain a list of users that can use the certificate
- Request revocation of the certificate if the subject is no longer accurate
- Request revocation of unexpired certificates if the organizational affiliation ends

### 3.2.3 Authentication of Individual Identity

#### *3.2.3.1 Authentication of Human Subscribers*

Updox requires remote identity proofing per DirectTrust LoA 3 for an individual acting as an:

1. Individual subscriber or
2. Organizational representative

Identity proofing is not performed on:

- Organization Information Security Officers (since Updox holds the private keys)
- Device sponsors (since Updox does not issue Device certificates)
- Patients (since Updox does not issue Patient certificates)

In its role as a Registration Authority, Updox

- Collects and verifies the following information with credit bureaus and applicable agencies:
  - Organization name
  - Organization address
  - Organization healthcare category
  - Organization taxpayer ID number (TIN)
  - Name of person whose identity is being verified
  - Home address
  - Date of birth
  - Work email address (not verified)
  - Government issued ID
    - Social Security Number or
    - Individual National Provider ID (NPI)
  - Financial or utility ID
    - Personal telephone number or
    - Financial knowledge question responses
- Assigns the Direct domain to ensure uniqueness and right to use
- Confirms the subscriber's ability to receive a telephone call at a number on file
- Records the subscriber's verbal attestation they are authorized to act on behalf of the organization (for domain-bound certificates)
- Verifies the legal existence of the organization (using the TIN)
- Requires the subscriber to accept the terms of the Updox Direct messaging user agreement which includes a requirement not to share their Direct messaging account with external parties/

#### *3.2.3.2 Authentication of Human Subscribers for Role-based Certificates*

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

#### *3.2.3.3 Authentication of Human Subscribers for Group Certificates*

A Group Certificate is a Certificate where the corresponding Private Key is shared by multiple entities. A DirectTrust certificate that is held and managed by Updox 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 section 3.2.2 and 3.2.3.1. Since Updox is the custodian of the certificates, the information identified in section 3.2.3.1 is also recorded for the Updox Information Systems Security Officer.

Additionally,

- The HISP Information Systems Security Officer or equivalent is responsible to ensure control of the private key.
- Subscribers do not hold or have access to the private key.

- The subjectName DN does not imply that the subject is a single individual.

In the case of a Direct Organizational Certificate, a Direct Address "User" is any human person that sends or receives a message via the Direct network on behalf of the Subscriber Organization. Identity validation for other users is performed by the Subscriber Organization which is bound through a legally binding contract to perform this function.
Prior to allowing a user access to the Direct network, the Subscriber Organization must:

- Collect the User's full legal name, an address of record, date of birth and an ID number (and ID type).
- Send the user's name to Updox.
- Provide the remaining information upon request by Updox

In addition, the Subscriber Organization must have processes in place that are sufficient to verify the User's identity at LoA3. The Subscriber Organization may be able to leverage its existing relationship as an employer or affiliate of a user to meet the identity verification requirements.

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

#### *3.2.3.4 Authentication of Devices*

Updox does not issue certificates for devices.

#### *3.2.3.5 Verification of NPI Number*

Updox does not include a National Provider Identifier in certificates issued.

### 3.2.4 Non-verified Subscriber Information

All Subscriber information included in the certificate is verified prior to issuing the certificate.

### 3.2.5 Validation of Authority

Updox, as the RA, verifies the association between an organization requesting an organization certificate and the individual representing the organization under the procedures outlined in section 3.2.2.

### 3.2.6 Criteria for Interoperation

Updox issues certificates according to the DirectTrust Certificate Policy.

## 3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

### 3.3.1 Identification and Authentication for Routine Re-key

Updox, as the CA, manages certificate re-keys on behalf of the Subscriber for use by the Updox HISP. The organizational and/or individual identity is based on the initial identify verification and the existing private key held by Updox.

### 3.3.2 Identification and Authentication for Re-key After Revocation

If a previously issued Updox certificate has been revoked the Subscriber must again go through the identify verification process described in section 3.2 to obtain a new certificate.

## 3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

Requests to revoke a certificate should be submitted via email to support@updox.com. An Updox representative will contact the requester and the customer, if different, to collect additional information and verify the validity and appropriateness of the request. Once validated, the certificate will be immediately revoked. The revoked certificate will be added to the CRL as notification to relying parties.

# 4 CERTIFICATE LIFE-CYCLE

## 4.1 APPLICATION

This section specifies requirements for the initial application for a Direct Trust certificate. It pertains to all certificate types issued by Updox (domain-bound and address-bound). Identity proofing is at LoA 3.

Updox is the RA, CA, and HISP for its Direct messaging service.

### 4.1.1 Submission of Certificate Application

All applicants must have an active Updox account. To submit a Direct messaging certificate application, the applicant completes the identity verification process described in section 3.2. Upon successful validation, Updox automatically issues the certificate.

### 4.1.2 Enrollment Process and Responsibilities

A Subscriber is responsible for providing accurate information about their organization and their self.

Updox ensures the identity of each applicant is verified in accordance with the Direct Trust CP and this CPS prior to issuing a certificate.

Updox authenticates and protects all communication made during the certificate application process.

## 4.2 CERTIFICATE APPLICATION PROCESSING

Updox, as the CA and RA, verifies that information in a certificate signing request is accurate and reflects the information presented by the Subscriber.

### 4.2.1 Performing Identification and Authentication Functions

The identity validation of Subscribers is performed by Updox as specified in section 3.2.

### 4.2.2 Approval or Rejection of Certificate Applications

Updox will approve a certificate application upon:

- Successful validation of the identity as specified in section 3.2
- Successful validation of the Subscriber application and
- Signed contract for Updox Direct services

Updox will reject a certificate application if:

- Identity validation fails
- Certificate signing request is incomplete or inaccurate
- Identifying information of any names in the certificate become invalid
- Private key is suspected of compromise
- Contract for Updox Direct services has not been signed
- Requested by the Subscriber
- Updox has reason to believe the Subscriber Organization is in violation of Direct agreements

### 4.2.3 Time to Process Certificate Applications

Updox normally issues a certificate immediately but no more than 5 days after completion of identity validation and verification of all Subscriber information placed in the certificate.

## 4.3 ISSUANCE

### 4.3.1 CA Actions During Certificate Issuance

Updox ensures that the public key is bound to the correct Subscriber then creates, issues, and publishes the certificate as specified in section 4.4.2 in a secure manner.

### 4.3.2 Notification to Subscriber of Certificate Issuance

Updox notifies the Subscriber applicant immediately during registration or via email when a certificate has been issued.

## 4.4 CERTIFICATE ACCEPTANCE

### 4.4.1 Conduct Constituting Certificate Acceptance

Use of a certificate by the Subscriber constitutes the Subscriber's acceptance of the certificate.

### 4.4.2 Publication of the Certificate by the CA

Updox publishes certificates as specified in section 2.2.1.

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

No stipulation.

## 4.5 KEY PAIR AND CERTIFICATE USAGE

### 4.5.1 Subscriber Private Key and Certificate Usage

Updox maintains the Private Key on behalf of the Subscriber, protects it from unauthorized access, and uses it only as specified by the *certificatePolicies* and *keyUsage* extensions in the certificate.

### 4.5.2 Relying Party Public Key and Certificate Usage

Certificates issued by Updox conform to the policies provided by the DirectTrust Certificate Policy. Relying parties should understand these policies. Updox publishes a certificate revocation list (CRL) as described in section 2.2.1. Relying parties should process the CRL on a regular basis and reject certificates found on it.

## 4.6 CERTIFICATE RENEWAL

Updox does not support certificate renewal. Instead, it relies on certificate re-key and posting of certificate information via the methods described in section 2.2.

### 4.6.1 Circumstance for Certificate Renewal

N/A

### 4.6.2 Who May Request Renewal

N/A

### 4.6.3 Processing Certificate Renewal Requests

N/A

### 4.6.4 Notification of New Certificate Issuance to Subscriber

N/A

### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

N/A

### 4.6.6 Publication of the Renewal Certificate by the CA

N/A

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

N/A

## 4.7 CERTIFICATE RE-KEY

Re-keying a certificate consists of creating new certificate with a different validity period, public key (and serial number) and signed with a different key. The remaining attributes remain the same. 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 is not revoked but will not be further re-keyed, renewed, or modified.

### 4.7.1 Circumstance for Certificate Re-key

To avoid interruption in service due to expiry, Updox will re-key the certificate before expiration (may also occur after a certificate expiration). Updox will also execute a certificate re-key at the request of an authorized party as specified in section 4.7.2. Updox will not re-key a revoked certificate.

### 4.7.2 Who May Request Certification of a New Public Key

Updox (as an RA and CA), the Subscriber, or their authorized representative may request the re-key of a Subscriber certificate.

### 4.7.3 Processing Certificate Re-keying Requests

Updox, as the CA, approves or rejects certificate re-keying requests. Identity verification of the Subscriber will 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

Updox, as the CA, does not support certificate modification instead certificates are re-keyed.

### 4.8.1 Circumstance for Certificate Modification

N/A

### 4.8.2 Who may request Certificate Modification

N/A

### 4.8.3 Processing Certificate Modification Requests

N/A

### 4.8.4 Notification of New Certificate Issuance to Subscriber

N/A

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

N/A

### 4.8.6 Publication of the Modified Certificate by the CA

N/A

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities

N/A

## 4.9 CERTIFICATE REVOCATION AND SUSPENSION

### 4.9.1 Circumstances for Revocation

Updox will revoke a certificate due to any of the following circumstances and publish the status in accordance with section 2.2:

- Private key is suspected of compromise
- Requested by the Subscriber
- Updox has reason to believe the Subscriber Organization is in violation of Direct agreements

### 4.9.2 Who Can Request Revocation

The following can request that a certificate be revoked:

- Updox employee as an agent of the RA and CA
- Subscriber or their authorized representative

### 4.9.3 Procedure for Revocation Request

A certificate revocation request identifies the certificate to be revoked by serial number and explains the reason for revocation. Updox will ensure the certificate revocation request is not malicious and will verify that the reason for revocation is valid. If the reason is valid, Updox will post the revocation on its CRL.

### 4.9.4 Revocation Request Grace Period

There is no grace period for revocation under the DirectTrust Certificate policy. Subscribers and authorized PKI entities may request the revocation of a certificate as soon as the need comes to their attention.

### 4.9.5 Time Within Which CA Must Process the Revocation Request

Updox will process all revocation requests within 8 hours of receipt.

### 4.9.6 Revocation Checking Requirement for Relying Parties

The matter of how often new revocation data should be obtained is to be determined by the Relying Party.

### 4.9.7 CRL Issuance Frequency

Updox issues and posts the CRL per the frequency specified in section 2.3.

### 4.9.8 Maximum Latency for CRLs

The maximum latency period for posting a CRL is within 4 hours of generation.

### 4.9.9 On-line Revocation/Status Checking Availability

N/A

### 4.9.10 On-line Revocation Checking Requirements

N/A

### 4.9.11 Other Forms of Revocation Advertisements Available

No other form of revocation is advertised.

### 4.9.12 Special Requirements Related to Key Compromise

Updox uses reasonable efforts to notify known Relying Parties if it discovers, or has reason to believe, there has been a compromise of Updox's private key.

### 4.9.13 Circumstances for Suspension

Updox does not support suspension of certificates.

### 4.9.14 Who Can Request Suspension

N/A

### 4.9.15 Procedure for Suspension Request

N/A

### 4.9.16 Limits on Suspension Period

N/A

## 4.10 CERTIFICATE STATUS SERVICES

Updox does not support certificate status services beyond a CRL.

#### 4.10.1 Operational Characteristics

N/A

#### 4.10.2 Service Availability

N/A

#### 4.10.3 Optional Features

N/A

### 4.11 End of Subscription

At the end of a subscription, the ability to send and receive Direct messages is removed (the certificate is left to expire).

### 4.12 Key Escrow and Recovery

Updox does not support key escrow and recovery for certificates.

#### 4.12.1 Key Escrow and Recovery Policy and Practices

N/A

#### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices

N/A

## 5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

### 5.1 Physical Controls

Updox hosts all technology necessary for support of this CPS in Updox's Data Centers (DCs). The DCs are SOC1 (SSAE 16) and SOC2 Type 2 audited, HIPAA and PCI compliant.

The DCs undergo external and internal audits against PCI, HIPAA, SOX, JSOX, GLB, NIST 800-53 based controls, SSAE 16, SOC 2 and many more standards. External Type II SSAE 16 SOC 1 and SOC 2 reports are prepared each year.

#### 5.1.1 Site Location and Construction

The off-site DCs have been purpose-built to support the continuous operation of hosted mission critical assets. The facilities have high-density, reinforced concrete walls encasing the data center core. The design and construction provide assurance that operations are protected against fire, floods, high winds, power outages, network issues and other hazards. The buildings are rated to withstand F3 tornados. There isn't any exterior signage.

### 5.1.2 Physical Access

The DCs have multiple layers of security, including video surveillance and biometric access control, to ensure that access is granted only to the appropriate individuals. Access is logged and retained. Each data center is protected and operated by an experienced network operations center (NOC) team.

### 5.1.3 Power and Air Conditioning

The DC has a fully redundant, 2(N+1) power, cooling, and network infrastructures. Power is provided by multiple power feeds from separate sources. Backup power is via multiple UPS devices and diesel-powered generator systems. The DCs also utilize multiple carrier-neutral, high-speed internet feeds, delivered over a secure and redundant network.

The DCs employ a cold-aisle containment system, as well as a mix of climate cooling and mechanical cooling to create reliable and efficient environmental conditions throughout the facilities.

### 5.1.4 Water Exposures

The DCs are located at geographic safe zones with 8-inch cement exterior walls to protect against water exposure.

### 5.1.5 Fire Prevention and Protection

All critical spaces in the data centers utilize a clean agent fire suppression system and are free of flammable materials. The entire data center structure has a dual-interlock pre-action sprinkler system. VESDA is utilized in the halls as well as in the return air plenums. Master fire panel resides in the data center Network Operations Center which is staffed 24x7. Central office monitoring is in place for all fire alerts.

### 5.1.6 Media Storage

Updox maintains a redundant architecture for all RA, CA, and HISP activities at two separate locations: 1) primary data center and 2) back-up data center. Updox does not utilize tape, disks, or any other type of mobile media.

### 5.1.7 Waste Disposal

Hardware and media are disposed of in accordance with HIPAA and industry best practices. Hard drives are destroyed before disposal, and shredding is used to dispose of documents and materials containing sensitive information.

## 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 are 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.

Updox has processes for screening and training these individuals as specified in section 5.3. Updox distributes its CA functions across four roles:

1. Administrator
2. Officer
3. Auditor
4. Operator

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
- Generating and backing up the CA keys

Administrators do not issue certificates to Subscribers.

#### *5.2.1.2 Officer*

The officer role is responsible for issuing certificates:

- Registering new Subscribers and requesting issuance of certificates
- Verifying the identity of Subscribers and accuracy of information included in certificates
- Approving and executing the issuance of certificates
- 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 Updox is operating in accordance with this CPS and the DirectTrust CP.

#### *5.2.1.4 Operator*

The operator role is responsible for:

- Routine operation of the CA equipment
- Performing operations such as system backups and recovery

### 5.2.2 Number of Persons Required Per Task

Updox trains at least two employees for each task, but only one employee is required to execute each task.

### 5.2.3 Identification and Authentication for Each Role

A person occupying a trusted role will be authenticated to the CA system.

### 5.2.4 Separation of Roles

Any authorized individual may assume the Operator role. No one individual will assume both the Officer and the Administrator roles.

## 5.3 PERSONNEL CONTROLS

### 5.3.1 Qualifications, Experience, and Clearance Requirements

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity. Preferred qualifications include bachelor's degree in Computer Science or similar, and 2+ years of experience in an information technology field. Persons who are not United States citizens are required to provide an H1b (non-immigrant visa).

### 5.3.2 Background Check Procedures

All employees must provide proper documentation for verification of identity and eligibility to work in the United States in accordance with the Federal Immigration Reform Act of 1986. A criminal background check is performed when onboarding a new workforce member.

### 5.3.3 Training Requirements

Persons in a trusted role receive training on the privacy, security, quality, and regulatory processes and procedures employed by Updox as well as a review of the PKI principles and operations. On-going training is based on the employee's role and is a continual part of each employee's development.

### 5.3.4 Retraining Frequency and Requirements

Retraining is on an as-needed basis (e.g. significant change to CA operations) to ensure personnel continue to meet the level of proficiency necessary to perform their job responsibilities competently.

### 5.3.5 Job Rotation Frequency and Sequence

No stipulation.

### 5.3.6 Sanctions for Unauthorized Sections

Any employee found to have performed unauthorized actions may be subject to disciplinary action, up to and including termination of employment.

### 5.3.7 Independent Contractor Requirements

Independent contractors are required to sign a non-disclosure agreement (NDA) and contract that requires compliance to the personnel requirements in this CPS.

### 5.3.8 Documentation Supplied to Personnel

Employees are provided documentation outlining their job responsibilities.

## 5.4 AUDIT LOGGING PROCEDURES

Audit log files are generated for events related to the RA and CA operations. All security audit logs are retained and made available during an audit.

### 5.4.1 Types of Events Recorded

All security auditing capabilities in the server operating system are enabled. The audit record includes:

- Type of event
- Date and time the event occurred
- A success or failure indicator, where appropriate
- Identity of the entity and/or person that caused the event

The following type of events are automatically recorded:

- Change to audit parameters (e.g. frequency, type of events audited)
- Attempt to delete or modify audit logs
- Attempt to assume a role (successful and unsuccessful)
- Change to maximum number of authentication attempts allowed
- Maximum number of unsuccessful authentication attempts reached during user login
- Unlock of an account locked by unsuccessful authentication
- Entry of security-relevant data
- Remote data entry of security-relevant messages received
- Export/output of confidential/security-relevant information (successful/unsuccessful)
- Generation of a key (not mandatory for one-time use keys)
- Loading of component private keys
- Access to certificate subject private keys
- Change to the trusted public keys (add, delete, edit)
- Manual entry of secret keys for authentication
- Export of private and secret keys
- Certificate request (new and re-key)
- Certificate issuance
- Change to the security configuration of a system component
- Change to user account (add, delete, edit)
- Change to user permissions

- Change to certificate profile
- Change to revocation profile
- Change to the certificate revocation list profile
- Third party time stamp is obtained
- Installation of a PKI application
- Installation of a hardware security module
- System start-up
- Logon attempts to PKI application
- Attempt to set/modify password
- Backup of internal database
- Restore from backup
- Re-key of the component
- Change to configuration – hardware
- Change to configuration – software
- Change to configuration – operating system
- Change to configuration – patches
- Software error condition
- Software check integrity failure
- Network attack (suspected or confirmed)
- Reset of operating system clock

The following type of events are manually recorded:

- Appointment of an individual to a Trusted Role
- Installation of an operating system
- Certificate revocation request
- Certificate compromise notification request
- Violation to physical security (known or suspected)
- Violation of Certificate Policy or Certificate Practices Statement
- System crash/hardware failure
- Equipment failure

### 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 Log

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

### 5.4.4 Protection of Audit Log

Only authorized staff have access and can archive the audit logs.

### 5.4.5 Audit Log Backup Procedures

Audit logs are backed up per section 5.1.8.

### 5.4.6 Audit Collection System (Internal vs. External)

Automated audit data is generated and recorded at the application level at all times while Updox is in operation.

### 5.4.7 Notification to Event-causing Subject

The subject is not notified of the audit event.

### 5.4.8 Vulnerability Assessments

Periodic vulnerability scans are conducted via 3rd party vendors.

## 5.5 RECORDS ARCHIVAL

### 5.5.1 Types of Records Archived

Records related to the certificate life-cycle detailed in section 4 are archived. This includes:

- CA accreditations
- CP and CPS
- Contractual obligations and other agreements regarding CA operations
- System and equipment configurations, modifications, and updates
- Certificate and revocation requests
- Identity validation
- Subscriber agreements
- Issued certificates
- Record of certificate re-keys
- CRLs
- Compliance auditor reports
- Changes to the CA audit parameters
- Attempts 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 actions taken as a result of violations of physical security
- Violations of the DirectTrust CP or Updox CPS

### 5.5.2 Retention Period for Archive

Archives are retained for a minimum of eight years.

### 5.5.3 Protection of Archive

Archives are protected according to the same requirements as specified in 5.4.4.

### 5.5.4 Archive Backup Procedures

No stipulation.

### 5.5.5 Requirements for Time-stamping of Records

Archive records are automatically time-stamped using a trusted time service as they are created.

### 5.5.6 Archive Collection System (Internal or External)

No stipulation.

### 5.5.7 Procedures to Obtain and Verify Archive Information

No stipulation.

## 5.6 KEY CHANGEOVER

Updox will not issue Subscriber certificates that extend beyond the expiration date of its own CA certificates and public keys. The CA certificate will be valid 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 will be retained and protected. Relying parties are notified by the addition or removal of CA certificates in the DirectTrust Accreditation Bundle.

The Updox self-signed root certificate is valid for no more than 20 years.

## 5.7 COMPROMISE AND DISASTER RECOVERY

### 5.7.1 Incident and Compromise Handling Procedures

Updox will investigate any incident suspected of compromising a certificate or resulting a disaster to determine the nature and the degree of damage.

If the CA key is suspected of compromise the procedures in Section 5.7.3 will be followed. Otherwise, the scope of potential damage will be assessed in order to determine if the CA certificate needs to be rebuilt, if only some certificates need to be revoked, and/or if the CA certificate key needs to be declared compromised.

If RA/CA equipment or software is damaged, operations will fail over to the backup data center. If RA/CA data is corrupted or lost, all information will be restored from backup or rebuilt as needed.

### 5.7.2 Computing Resources, Software, and/or Data are Corrupted

Updox maintains backup copies of system, databases, and private keys in order to rebuild the RA/CA capabilities in case of software and/or data corruption. Prior to resuming operations, Updox will ensure that the system's integrity has been restored.

### 5.7.3 Entity Private Key Compromise Procedures

If the Updox 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 PKI management capability is damaged and inoperative, Updox will reestablish operations as quickly as possible per the Contingency Plan policy, giving priority to the ability to revoke Subscriber's certificates.

In the case of a disaster whereby both Updox CA installations are physically damaged and all copies of the CA signature key are destroyed as a result, Updox will be completely rebuilt by reestablishing the CA equipment and generating new key pairs. All Subscriber Certificates will 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 OR RA TERMINATION

In the event of Updox CA termination, certificates signed by Updox will be revoked. In the event of Updox RA termination, another RA service will be retained. In either event, relying parties will be notified as needed.

# 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 is generated by software that is well protected according to the physical controls in section 6.2.1.

#### *6.1.1.2 Subscriber Key Pair Generation*

The CA cryptographic keying material generated for Subscriber certificates is created by software hardware that is well protected according to the physical controls in section 6.2.1.

### 6.1.2 Private Key Delivery to Subscriber

Private Keys are not distributed to the Subscriber; rather Updox creates, stores, and manages the key pairs.

### 6.1.3 Public Key Delivery to Certificate Issuer

Updox holds the Public Keys.

### 6.1.4 CA Public Key Delivery to Relying Parties

The Updox CA root public key is delivered within a self-signed certificate using reasonable out-of-band medium trusted (e.g. DirectTrust Accredited Bundle) by the relying party.

### 6.1.5 Key sizes

Updox utilizes the SHA-256 algorithm for all certificate signatures. Key size is at least 2048 bits (RSA).

### 6.1.6 Public Key Parameters Generation and Quality Checking

Updox generates Public Key parameters for signature algorithms and performs parameter quality checking in accordance with FIPS 186.

### 6.1.7 Key Usage Purposes

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

- digitalSignature
- keyEncipherment

Updox Subscriber certificates:

- assert key usages based on the intended application of the key pair
- do not assert the non-repudiation bit
- assert a Basic Constraint of CA: FALSE
- assert an extended key usage bit of *emailProtection*
- are dual-use certificates

The Updox CA root certificate asserts:

- key usage bit: cRLSign
- key usage bit: keyCertSign
- Basic Constraint of CA:TRUE

## 6.2 Private Key Protection and Cryptographic Module Engineering Controls

### 6.2.1 Cryptographic Module Standards and Controls

Cryptographic modules are compliant with FIPS 140 Level 2:

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

No stipulation.

### 6.2.3 Private Key Escrow

Private keys are not escrowed.

### 6.2.4 Private Key Backup

The private keys are backed up regularly and a copy also stored offsite to facilitate disaster recovery.

### 6.2.5 Private Key Archival

No stipulation.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

If transferred, private keys will be maintained in a cryptographic module meeting the requirements in section 6.2.1 as applicable. Private keys will not exist in the clear outside of a cryptographic module.

### 6.2.7 Private Key Storage on Cryptographic Module

Private Keys are stored in a cryptographic module meeting the requirements in section 6.2.1 as applicable.

### 6.2.8 Method of Activating Private Key

Private keys are activated by default when generated.

### 6.2.9 Method of Deactivating Private Key

Updox deactivates private keys when not in use and prevents unauthorized access its cryptographic module.

### 6.2.10 Method of Destroying Private Key

Updox automatically destroys private keys upon expiration and revocation as specified in section 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

The Updox CA self-signed certificate and the associated private key are used for a maximum of 20 years. Subscriber public and private keys are used for a maximum of 3 years.

## 6.4 ACTIVATION DATA

### 6.4.1 Activation Data Generation and Installation

Not applicable since Updox holds the private keys on behalf of the Subscriber.

### 6.4.2 Activation Data Protection

Not applicable since Updox holds the private keys on behalf of the Subscriber.

### 6.4.3 Other Aspects of Activation Data

No stipulation.

## 6.5 COMPUTER SECURITY CONTROLS

### 6.5.1 Specific Computer Security Technical Requirements

Updox configures its CA systems, including any remote workstations, to:

- Authenticate the identity of user before permitting access to the system or applications
- Manage the privileges of users and limit users to their assigned roles
- Generate and archive audit records
- Enforce domain integrity boundaries for security critical processes
- Support recovery from key or system failure

### 6.5.2 Computer Security Rating

No stipulation.

## 6.6 LIFE CYCLE TECHNICAL CONTROLS

### 6.6.1 System Development Controls

Updox develops in a controlled development environment with modern source code control. CA hardware and software are dedicated to performing the CA tasks. CA hardware and software containing private keys are well protected. Hardware and software updates are tested and installed in a professional and controlled manner.

### 6.6.2 Security Management Controls

Updox requires all changes to be evaluated, documented, and approved before implementation.

### 6.6.3 Life Cycle Security Controls

No stipulation.

## 6.7 NETWORK SECURITY CONTROLS

Information transferred from Updox is done through secure networks per the Updox Security Policy. Updox employs security measures to ensure it is guarded against denial of service and intrusion attacks which includes firewalls and filtering routers.

## 6.8 TIME-STAMPING

Updox system clocks are synchronized with the NIST national time protocol servers (time-a-g.nist.gov, time-a-wwv.nist.gov, time-a-b.nist.gov, utcnist.colorado.edu). The Updox system clocks are accurate within five seconds of the NIST time service and synchronization occurs every 64 to 1024 seconds.

# 7 CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 CERTIFICATE PROFILE

### 7.1.1 Version Numbers

Updox issues X.509 version 3 certificates, indicated by the version field = 2.

### 7.1.2 Certificate Extensions

Certificates leverage the following extensions in compliance with RFC 5280:

- The Key Usage, Extended Key Usage, and Basic Constraints extensions are populated as specified in section 6.1.7
- The CRL Distribution Points extension is populated with a CRL URI as specified in section 2.2
- The Subject Alternative Name extension is populated as specified in section 3.1.1
- The Certificate Policies extension is populated as specified in section 7.1
- The non-repudiation flag is not set in the certificate

### 7.1.3 Algorithm Object Identifiers

End entity certificates use the SHA-256 signature algorithm:
sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates 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.

### 7.1.5 Name Constraints

No stipulation.

### 7.1.6 Certificate Policy Object Identifier

As per section 1.2, Updox asserts in the *certificatePolicies* extension of the certificate an OID for each of the following:

- DirectTrust Certificate Policy
- Identity proofing Level of Assurance
- Healthcare category of the Subscriber

### 7.1.7 Usage of Policy Constraints Extension

No stipulation

#### 7.1.8 Policy Qualifiers Syntax and Semantics

The Certificate Policy Extension field is populated in certificates as specified in section 1.2.

#### 7.1.9 Processing Semantics for the Critical Certificate Policies Extension

The *certificatePolicies* extension is a non-critical extension, however, Relying Parties whose client software does not process this extension risk using certificates inappropriately.

### 7.2 CRL PROFILE

#### 7.2.1 Version Number(s)

Updox issues X.509 version 2 CRLs, as indicated by the version field = 1.

#### 7.2.2 CRL and CRL Entry Extensions

Updox conforms to the CRL and CRL Extensions profile defined in IETF RFA 5280.

The CRL is signed using the sha-256 signature algorithm and identified by the OID:
sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

The CRL contains a CRL Reason Code entry extension for each entry.

### 7.3 OCSP PROFILE

Updox has not deployed an OSCP responder.

#### 7.3.1 Version Number(s)

N/A

#### 7.3.2 OCSP Extensions

N/A

## 8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

In addition to internal reviews, Updox contracts with the following 3rd party assessors to help ensure the requirements specified by the Direct Project, this CPS, and the DirectTrust CP are implemented and enforced.

- EHNAC Accreditation (HISP Privacy and Security)
- DirectTrust RA, CA, and HISP Accreditation
- ONC Health IT Certification
- Cadre Security Assessment
- Updox 3rd party Data Centers undergo SOC1 (SSAE 16) and SOC2 Type 2 audits.

## 8.1 FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

| | | |
|---|---|---|
| EHNAC | Bi-annual | Covers security and HIPAA policies |
| DirectTrust | Bi-annual | Covers RA, CA, and HISP functions |
| ONC Health IT | Bi-annual | Covers Direct messaging transport and cert discovery |
| Cadre Security | Annual | Covers network security |
| Data Centers | Annual | SOC1 (SSAE 16) and SOC2 Type 2 audits. |

## 8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR

The independent auditor must:

- Demonstrate competence in the field of compliance audits
- Be familiar with Public Key infrastructures, certification systems, and Internet security issues

## 8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

Updox uses independent auditors that do not have a financial interest with Updox.

## 8.4 TOPICS COVERED BY ASSESSMENT

The assessment includes but is not limited to the following:

- Site Description
- Network Security
- Physical Security
- Commitment to Quality
- Risk Management
- Control Activities
- Monitoring
- Information and Communication
- HIPAA Policies

## 8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports a material noncompliance with applicable law or this CPS then Updox will initiate a formal action plan to remediate the deficiencies.

## 8.6 COMMUNICATION OF RESULTS

The results of each audit are reported to the Updox Management Team for review and approval. DirectTrust is notified of EHNAC accreditation status.

# 9 OTHER BUSINESS AND LEGAL MATTERS

## 9.1 FEES

### 9.1.1 Certificate Issuance or Renewal fees

The fees set forth in the Subscriber Agreement include certificate issuance and renewal fees.

### 9.1.2 Certificate Access Fees

Updox does not charge for access and use of the certificates by Relying Parties. The fees set forth in the Subscriber Agreement include fees for access to a certificate by a Subscriber.

### 9.1.3 Revocation or Status Information Access Fees

Updox does not charge a fee for access to revocation or status information using the methods indicated in section 2.2.

### 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

Updox maintains commercial general liability insurance of not less than $5,000,000 in aggregate.

The Subscriber is encouraged to maintain commercially reasonable levels of the following types of insurance: (i) commercial general liability, (ii) errors and omissions liability, (iii) worker's compensation, and (iv) network security, privacy protection and notification coverage.

### 9.2.2 Other Assets

No stipulation.

### 9.2.3 Insurance or Warranty Coverage for End-entities

No stipulation.

## 9.3 CONFIDENTIALITY OF BUSINESS INFORMATION

### 9.3.1 Scope of Confidential Information

Confidential Information means any information that (a) is clearly marked as confidential, (b) that by its nature or context should reasonably be understood to be confidential, and (c) the information specifically set forth in the list below.

- Subscriber applications
- Audit logs for types specified in section 5.4.1
- Updox policies and procedures related to this CPS
- Audit reports and related documentation

### 9.3.2 Information not Within the Scope of Confidential Information

Confidential Information will not include any information (i) that is publicly available through no breach of this CPS, (ii) that is independently developed by Subscriber, Updox, or (iii) that is rightfully acquired by Subscriber or Updox from a third party who is not in breach of an agreement to keep such information confidential. Except as expressly permitted by this CPS, neither Subscriber or Updox will disclose, use, copy, distribute, sell, license, publish, reproduce or otherwise make available confidential information of others.

### 9.3.3 Responsibility to Protect Confidential Information

Updox and Subscriber will each (i) secure and protect confidential information by using the same or greater level of care that it uses to protect its own confidential and proprietary information of like kind, but in no event less than a reasonable degree of care, and (ii) require that each of their respective employees, agents, attorneys and independent contractors who have access to such confidential information are bound to at least as restrictive confidentiality terms as this section 9.3.

Notwithstanding the foregoing, any party may disclose another party's confidential information to the extent required by applicable law or regulation or by order of a court or other governmental entity, in which case, if permitted, such party will notify the other disclosing party as soon as practicable prior to such party making such required disclosure.

## 9.4 PRIVACY OF PERSONAL INFORMATION

### 9.4.1 Privacy Plan

Updox protects the privacy of the information sent through Updox Direct in accordance with its privacy policy which can be found at http://updox.com/privacy-policy.

### 9.4.2 Information Treated as Private

See section 9.3.1.

### 9.4.3 Information not Deemed Private

See section 9.3.2.

### 9.4.4 Responsibility to Protect Private Information

Private information is stored securely according to this CPS.

### 9.4.5 Notice and Consent to Use Private Information

Private information may be used by Updox in accordance with this CPS, the privacy policy referenced in section 9.4.1, the BAA, and applicable Subscriber Agreements.

### 9.4.6 Disclosure Pursuant to Judicial or Administrative Process

Notwithstanding the foregoing, Updox may disclose confidential and/or private information to the extent required by applicable law or regulation or by order of a court or other governmental entity, in which case, if permitted, Updox will notify the disclosing party as soon as practicable prior to such party making such required disclosure.

### 9.4.7 Other Information Disclosure Circumstances

No stipulation.

## 9.5 INTELLECTUAL PROPERTY RIGHTS

Updox has and will retain sole and exclusive right, title and interest, including copyright and all other rights, in and for the Updox Direct services. Updox hereby reserves all rights not expressly granted hereunder. Updox will not knowingly violate the intellectual property rights held by others.

## 9.6 REPRESENTATIONS AND WARRANTIES

### 9.6.1 CA Representations and Warranties

Updox warrants that it will perform the functions outlined in this CPS in accordance with applicable laws and regulations and in a professional manner.

### 9.6.2 RA Representations and Warranties

Updox warrants that:

- The information provided within the certificate is true and correct
- It has completed required identity verification as set forth in section 3
- It performs the functions of an RA and CA in a professional manner and in accordance with applicable laws and regulations, and with this CPS

### 9.6.3 Subscriber Representations and Warranties

Subscriber warrants it will:

- Limit users to only employees or affiliates of the organization named in the certificate subject
- Provide accurate and complete information to Updox
- Assert identity verification has been completed as set forth in section 3
- Confirm the accuracy of certificate data prior to using the certificate

- Promptly cease using a certificate and notify Updox if (i) any information that was submitted to Updox becomes misleading or (ii) there is any actual or suspected misuse or compromise of the private key associated with the certificate
- Use the certificate only for authorized and legal purposes, consistent with this CPS and Subscriber Agreement
- Promptly cease using the certificate and related Private Key after the certificate's expiration

#### 9.6.4 Relying Party Representations and Warranties

Relying Party warrants that:

- It will only use certificates for the purpose for which they were intended, and for no other purposes whatsoever, and in compliance with all applicable laws and regulations, and this CPS
- It will check each certificate for validity and authenticity
- It will promptly notify Updox of any issues or problems with a certificate of which it becomes aware
- Its decision to rely on the information within a certificate is solely its responsibility

#### 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

Updox expressly disclaims all other warranties, both express and implied. Specifically, and without limitation, Updox does not warrant that the Updox Direct services will be error-free or uninterrupted or that any defects will be corrected. There are no implied warranties of accuracy, merchantability and fitness for a particular purpose, non-infringement of proprietary rights or any other warranty as may otherwise be applicable to the Updox Direct services.

## 9.8 LIMITATIONS OF LIABILITY

To the maximum extent permitted by law, Updox will not be liable under this CPS for lost revenues or direct, indirect, special, incidental, consequential, exemplary, or punitive damages, even if the claimant knew or should have known that such damages were possible and even if direct damages do not satisfy a remedy.

## 9.9 INDEMNITIES

To the extent permitted by applicable law, the Subscriber agrees to indemnify, defend and hold Updox harmless from and against all claims brought by a third party against Updox which arise out of or are related to:

- Subscriber's breach of its obligations under or the terms of this CPS
- Its use of Updox Direct, other than those claims arising out of or related to the CA's negligence or willful misconduct in providing Updox Direct

Additional indemnities may be found in the Subscriber Agreement.

## 9.10 TERM AND TERMINATION

### 9.10.1 Term

Upon publication, the CPS is effective immediately and supersedes all prior versions.

### 9.10.2 Termination

Termination of this CPS may occur if approved by the Updox management team.

### 9.10.3 Effect of Termination and Survival

The requirements of this CPS remain in effect through the validity period for all certificates issued by Updox.

## 9.11 INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

Notices will be given in commercially reasonable manner, as dictated by the circumstance.

## 9.12 AMENDMENTS

### 9.12.1 Procedure for Amendment

This CPS may be amended by the Updox management team as needed.

### 9.12.2 Notification Mechanism and Period

No stipulation.

### 9.12.3 Circumstances Under Which OID Must be Changed

When DirectTrust deems a change to its Certificate policy is substantive, Updox will make a corresponding change to the policy OID expressed in the certificates.

## 9.13 DISPUTE RESOLUTION PROVISIONS

If a dispute arises, Updox will first attempt to resolve the issue with the other party. If unsuccessful, Updox will then attempt to resolve the dispute through DirectTrust before resorting to adjudication through the court system. Any cause of action or claim against Updox under this CPS must be commenced within one (1) year after the claim or cause of action arises.

## 9.14 GOVERNING LAW

This CPS is governed by the laws of the United States of America.

## 9.15 COMPLIANCE WITH APPLICABLE LAW

This CPS is subject to applicable federal, state, and local laws, rules, and regulations. Updox, each Subscriber, and Relying Party will comply with all of these laws, as it relates to their responsibilities hereunder.

## 9.16 MISCELLANEOUS PROVISIONS

### 9.16.1 Entire Agreement

This CPS constitutes the entire agreement related to the subjects herein and supersedes all prior or contemporaneous agreements, representations and proposals, written or oral, if any, regarding such subjects.

### 9.16.2 Assignment

No certificate issued under this CPS may be assigned without prior written approval of Updox. Updox may assign its rights and obligations under this CPS in its sole discretion.

### 9.16.3 Severability

If any provision hereof is held to be invalid or unenforceable, the remaining provisions will remain in full force. All waivers of and consents to any terms of this CPS (or any rights, powers or remedies under it) must be in writing to be effective. No waiver or consent granted for one matter will be construed as a waiver or consent for a different matter.

### 9.16.4 Enforcement (Attorney Fees/Waiver of Rights)

No stipulation.

### 9.16.5 Force Majeure

Updox will not be liable for failure to perform any of its obligations under this CPS if such failure is caused by an event outside its reasonable control, including but not limited to, an act of God, war, an act of terrorism, fire, or natural disaster.

## 9.17 OTHER PROVISIONS

No stipulation.

# Document History

| Date | Description | By |
|---|---|---|
| 06/09/2015 | CPS updated to correspond with DirectTrust CP 1.2 and approved by Updox Management Team. | Connie Patterson |
| 08/12/2015 | Rewrote sections 1.1, 1.2, 3.2, and 3.2.3.1, added patient identity verification to section 3.2.3.1, and made minor cosmetic changes. | Connie Patterson |
| 12/29/2015 | Rewrote the Healthcare Category paragraph in section 3.2.2. | Connie Patterson |
| 07/10/2017 | Updated CPS to comply with DirectTrust Policy 3.1. | Connie Patterson |
| 07/12/2017 | CPS 1.3 approved by management team | Connie Patterson |
| 5/16/2018 | Updated the Updox corporate office address, logo, modified information regarding the data center facilities, and corrected a few minor typos. | Connie Patterson |
| 10/18/2018 | Modified section 4.11 | Connie Patterson |
| 05/01/2019 | Changed version # to 1.4<br>Section 1.1.4 - added<br>Section 1.2 – updated the CP and LoA OIDs<br>Section 1.3.2.1 – added<br>Section 1.3.3.1 – added<br>Section 1.3.5.2 – added<br>Section 1.6.2 – added Affiliated Organization, Custodian, NPI<br>Section 2.2.1 – updated CRL to version 1.4<br>Section 2.2.1 – updated CPS to version 1.4<br>Section 3.1.1 – Common Name updated to version 1.4<br>Section 3.2.3.5 – added<br>Section 9.2.1 – updated insurance to $5M<br>Section 9.4.3 - added<br>Section 9.6.5 - added | Connie Patterson |
| 10/30/2019 | Section 3.2 – added more detail on the healthcare category, legal existence, etc.<br>Section 3.4 – added more detail on the revocation process<br>Section 4.1.1 – added more detail on the certificate application process<br>Section 5.6 – added detail on how relying parties are notified<br>Section 5.7 – reworded for clarification<br>Section 5.8 – added more detail on RA/CA termination<br>Section 6.8 – added the specific NIST time servers<br>Section 8.1 – changed RA & CA accreditation to DirectTrust | Connie Patterson |