



**SURESCRIPTS CA**  
**CERTIFICATION PRACTICE STATEMENT**

**DATE: 2/22/2017**

## DOCUMENT CHANGE LOG

Version	Date	Details
1.0	03.21.2013	Whole doc
1.0.a	04.25.2013	Whole doc
2.0	03.13.2014	Formatting, Ownership and contact information, and updates to IDP processes
3.0	09.28.2015	Combined in practices for issuing TLS certificates under Federal Bridge program and Webtrust 2.0
3.0a	10.09.2015	Updated subscriber requirements and subscriber document retention
3.1	11,11.2015	Updated certificate revocation procedures
3.2	1.30.2017	Updated OID, HISP policy reference, contact information
3.3	2/22/2017	Updates for SSL Baseline changes in Dec 2016 for Webtrust

## **SURESCRIPTS CPS**

PUBLISHED BY  
SURESCRIPTS, L.L.C.  
920 2ND AVENUE S.  
MINNEAPOLIS, MN 55402  
PHONE: 866-267-9482  
FAX: 651-855-3001

2800 CRYSTAL DRIVE  
ARLINGTON, VA 22202  
PHONE: 866-797-3239  
FAX: 703-921-2191

## Proprietary and Confidential

This document is proprietary information of Surescripts and may not be reproduced or distributed without the express written consent of Surescripts

# TABLE OF CONTENTS

SECTION 1	Introduction .....	1
1.1	Overview.....	1
1.1.1	Certificate Policy (CP) .....	1
1.1.2	Relationship between the Surescripts CPS and the DirectTrust Community X.509 Certificate Policy .....	2
1.1.3	Relationship between the Surescripts CPS and DirectTrust HISP Policy.....	2
1.2	Document Name and Identification .....	2
1.3	PKI Participants .....	3
1.3.1	PKI Authorities.....	4
1.3.2	Certification Authorities.....	4
1.3.3	Registration Authorities .....	5
1.3.4	Subscribers, Subjects and Applicants .....	5
1.3.5	Health Information Service Providers (HISPs) .....	5
1.3.6	Relying Parties .....	5
1.3.7	Operational Authority (OA) .....	5
1.3.8	Other Participants.....	6
1.4	Certificate Usage .....	6
1.4.1	Appropriate Certificate Uses .....	6
1.4.2	Prohibited Certificate Uses .....	6
1.5	Policy Administration .....	6
1.5.1	Organization Administering the Document.....	6
1.5.2	Contact Person.....	7
1.5.3	Person Determining CPS Suitability for the Certificate Policy.....	7
1.5.4	Certification Practice Statement Approval Procedures .....	7
1.6	Definitions and Acronyms.....	7
SECTION 2	Publication and Repository Responsibilities .....	11
2.1	Repositories.....	11
2.1.1	Repository Obligations .....	11
2.2	Publication of Certification Information.....	11
2.2.1	Publication of Certificates and Certificate Status .....	11
2.2.2	Publication of CA Information .....	11
2.2.3	Interoperability .....	12
2.3	Frequency of Publication .....	12
2.4	Access Controls on Repositories .....	12
SECTION 3	Identification and Authentication.....	13
3.1	Naming .....	13
3.1.1	Types of Names .....	13
3.1.2	Need for Names to be Meaningful.....	13
3.1.3	Anonymity or Pseudonymity of Subscribers.....	13
3.1.4	Rules for Interpreting Various Name Forms.....	13
3.1.5	Uniqueness of Names .....	13
3.1.6	Recognition, Authentication, and Role of Trademarks.....	14

3.2	Initial Identity Validation.....	14
3.2.1	Method to Prove Possession of Private Key .....	14
3.2.2	Authentication of Organization Identity.....	14
3.2.3	Authentication of Individual Identity .....	17
3.2.4	Non-verified Subscriber Information.....	20
3.2.5	Validation of Authority.....	21
3.2.6	Criteria for Interoperation.....	21
3.3	Identification and Authentication for Re-key Requests .....	21
3.3.1	Identification and Authentication for Routine Re-key .....	21
3.3.2	Identification and Authentication for Re-key after Revocation .....	21
3.4	Identification and Authentication for Revocation Request.....	21
SECTION 4	Certificate Life-Cycle .....	22
4.1	Application .....	22
4.1.1	Submission of Certificate Application .....	22
4.1.2	Enrollment Process and Responsibilities .....	22
4.2	Certificate Application Processing.....	22
4.2.1	Performing Identification and Authentication Functions.....	22
4.2.2	Approval or Rejection of Certificate Applications .....	22
4.2.3	Time to Process Certification Applications .....	23
4.3	Issuance .....	23
4.3.1	CA Actions During Certificate Issuance .....	23
4.3.2	Notification to Subscriber of Certificate Issuance.....	23
4.4	Certificate Acceptance.....	23
4.4.1	Conduct Constituting Certificate Acceptance .....	23
4.4.2	Publication of the Certificate by the CA.....	23
4.4.3	Notification of Certificate Issuance by the CA to Other Entities .....	23
4.5	Key Pair and Certificate Usage .....	24
4.5.1	Subscriber Private Key and Certificate Usage .....	24
4.5.2	Relying Party Public Key and Certificate Usage .....	24
4.6	Certificate Renewal .....	24
4.6.1	Circumstance for Certificate Renewal .....	24
4.6.2	Who May Request Renewal .....	24
4.6.3	Processing Certificate Renewal Requests .....	24
4.6.4	Notification of New Certificate Issuance to Subscriber .....	24
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate.....	24
4.6.6	Publication of the Renewal Certificate by the CA.....	25
4.6.7	Notification of Certificate Issuance by the CA to Other Entities .....	25
4.7	Certificate Re-Key .....	25
4.7.1	Circumstance for Certificate Re-Key .....	25
4.7.2	Who May Request Certification of a New Public Key .....	25
4.7.3	Processing Certificate Re-Keying Requests .....	25
4.7.4	Notification of New Certificate Issuance to Subscriber .....	25
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate.....	25
4.7.6	Publication of the Re-keyed Certificate by the CA .....	26

---

4.7.7	Notification of Certificate Issuance by the CA to Other Entities .....	26
4.8	Modification .....	26
4.8.1	Circumstance for Certificate Modification .....	26
4.8.2	Who May Request Certificate Modification .....	26
4.8.3	Processing Certificate Modification Requests .....	26
4.8.4	Notification of New Certificate Issuance to Subscriber .....	26
4.8.5	Conduct Constituting Acceptance of Modified Certificate .....	26
4.8.6	Publication of the Modified Certificate by the CA .....	26
4.8.7	Notification of Certificate Issuance by the CA to Other Entities .....	26
4.9	Certificate Revocation and Suspension .....	27
4.9.1	Circumstances for Revocation .....	27
4.9.2	Who Can Request Revocation .....	27
4.9.3	Procedure for Revocation Request .....	27
4.9.4	Revocation Request Grace Period .....	27
4.9.5	Time Within Which CA Must Process the Revocation Request .....	28
4.9.6	Revocation Checking Requirements for Relying Parties .....	28
4.9.7	CRL Issuance Frequency .....	28
4.9.8	Maximum Latency of CRLs .....	28
4.9.9	On-Line Revocation/Status Checking Availability .....	28
4.9.10	On-Line Revocation Checking Requirements .....	28
4.9.11	Other Forms of Revocation Advertisements Available .....	28
4.9.12	Special Requirements Related to Key Compromise .....	29
4.9.13	Circumstances for Suspension .....	29
4.9.14	Who Can Request Suspension .....	29
4.9.15	Procedure for Suspension Request .....	29
4.9.16	Limits on Suspension Period .....	29
4.10	Certificate Status Services .....	29
4.10.1	Operational Characteristics .....	29
4.10.2	Service Availability .....	29
4.10.3	Optional Features .....	29
4.11	End of Subscription .....	29
4.12	Key Escrow and Recovery .....	30
4.12.1	Key Escrow and Recovery Policy and Practices .....	30
4.12.2	Session Key Encapsulation and Recovery Policy and Practices .....	30
<b>SECTION 5</b>	<b>Facility Management and Operations Controls .....</b>	<b>31</b>
5.1	Physical Controls .....	31
5.1.1	Site Location and Construction .....	31
5.1.2	Physical Access .....	31
5.1.3	Power and Air Conditioning .....	31
5.1.4	Water Exposures .....	31
5.1.5	Fire Prevention and Protection .....	32
5.1.6	Media Storage .....	32
5.1.7	Waste Disposal .....	32
5.1.8	Off-Site Backup .....	32

---

5.2	Procedural Controls .....	32
5.2.1	Trusted Roles .....	32
5.2.2	Number of Persons Required Per Task .....	33
5.2.3	Identification and Authentication for Each Role .....	34
5.2.4	Separation of Roles .....	36
5.3	Personnel Controls .....	36
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements ....	36
5.3.2	Background Check Procedures.....	37
5.3.3	Training Requirements .....	37
5.3.4	Job Rotation Frequency and Sequence .....	37
5.3.5	Sanctions for Unauthorized Actions .....	37
5.3.6	Independent Contractor Requirements .....	38
5.3.7	Documentation Supplied to Personnel .....	38
5.4	Audit Logging Procedures .....	38
5.4.1	Types of Events Recorded .....	38
5.4.2	Frequency of Processing Log.....	41
5.4.3	Retention Period for Audit Logs .....	41
5.4.4	Protection of Audit Logs .....	41
5.4.5	Audit Log Backup Procedures .....	42
5.4.6	Audit Collection System (internal vs. external).....	42
5.4.7	Notification to Event-Causing Subject .....	42
5.4.8	Vulnerability Assessments.....	42
5.5	Records Archival .....	42
5.5.1	Types of Events Archived.....	42
5.5.2	Retention Period for Archive.....	43
5.5.3	Protection of Archive .....	43
5.5.4	Archive Backup Procedures .....	43
5.5.5	Requirements for Time-Stamping of Records .....	44
5.5.6	Archive Collection System (Internal vs. External) .....	44
5.5.7	Procedures to Obtain & Verify Archive Information.....	44
5.6	Key Changeover.....	44
5.7	Compromise and Disaster Recovery.....	44
5.7.1	Incident and Compromise Handling Procedures.....	44
5.7.2	Computing Resources, Software, and/or Data Are Corrupted .....	45
5.7.3	Entity Private Key Compromise Procedures .....	45
5.7.4	Business Continuity Capabilities after a Disaster.....	45
5.8	CA and RA Termination.....	46
SECTION 6	Technical Security Controls.....	47
6.1	Key Pair Generation and Installation.....	47
6.1.1	Key Pair Generation .....	47
6.1.2	Private Key Delivery to Subscriber .....	47
6.1.3	Public Key Delivery to Certificate Issuer .....	47
6.1.4	CA Public Key Delivery to Relying Parties .....	47
6.1.5	Key Sizes	47

6.1.6	Public Key Parameters Generation and Quality Checking.....	48
6.1.7	Key Usage Purposes (as per X.509 v3 key usage field).....	48
6.2	Private Key Protection and Cryptographic Module Engineering Controls.....	49
6.2.1	Cryptographic Module Standards and Controls .....	49
6.2.2	Private Key (n out of m) Multi-person Control .....	50
6.2.3	Private Key Escrow .....	50
6.2.4	Private Key Backup .....	50
6.2.5	Private Key Archival .....	50
6.2.6	Private Key Transfer into or from a Cryptographic Module .....	50
6.2.7	Private Key Storage on Cryptographic Module .....	50
6.2.8	Method of Activating Private Keys.....	50
6.2.9	Methods of Deactivating Private Keys.....	50
6.2.10	Method of Destroying Private Keys .....	50
6.2.11	Cryptographic Module Rating.....	51
6.3	Other Aspects of Key Management .....	51
6.3.1	Public Key Archival.....	51
6.3.2	Certificate Operational Periods/Key Usage Periods .....	51
6.4	Activation Data .....	52
6.4.1	Activation Data Generation and Installation .....	52
6.4.2	Activation Data Protection .....	52
6.4.3	Other Aspects of Activation Data .....	52
6.5	Computer Security Controls .....	52
6.5.1	Specific Computer Security Technical Requirements .....	52
6.5.2	Computer Security Rating .....	53
6.6	Life-Cycle Security Controls .....	53
6.6.1	System Development Controls.....	53
6.6.2	Security Management Controls.....	53
6.6.3	Life Cycle Security Ratings.....	53
6.7	Network Security Controls.....	54
6.8	Stamping.....	54
SECTION 7	Certificate, CRL, and OCSP Profile Formats .....	55
7.1	Certificate Profile .....	55
7.1.1	Version Numbers.....	55
7.1.2	Certificate Extensions.....	55
7.1.3	Algorithm Object Identifiers .....	55
7.1.4	Name Forms.....	56
7.1.5	Name Constraints.....	56
7.1.6	Certificate Policy Object Identifier .....	56
7.1.7	Usage of Policy Constraints Extension .....	56
7.1.8	Policy Qualifiers Syntax and Semantics.....	56
7.1.9	Processing Semantics for the Critical Certificate Policy Extension.....	56
7.2	CRL Profile .....	56
7.2.1	Version Numbers.....	56
7.2.2	CRL and CRL Entry Extensions .....	56



---

7.3	OCSP Profile .....	57
<b>SECTION 8</b>	<b>Compliance Audits and Other Assessments.....</b>	<b>58</b>
8.1	Independent Audit for PKI operation .....	58
8.2	Identity/Qualifications of Assessor .....	58
8.3	Assessor's Relationship to Assessed Entity.....	58
8.4	Topics Covered by Assessment.....	59
8.5	Actions Taken as a Result of Deficiency .....	59
8.6	Communication of Results.....	59
<b>SECTION 9</b>	<b>Other Business and Legal Matters .....</b>	<b>60</b>
9.1	Fees.....	60
9.1.1	Certificate Issuance/Renewal Fees .....	60
9.1.2	Certificate Access Fees.....	60
9.1.3	Revocation or Status Information Access Fee .....	60
9.1.4	Fees for other Services .....	60
9.1.5	Refund Policy .....	60
9.2	Financial Responsibility .....	60
9.2.1	Insurance Coverage .....	60
9.2.2	Other Assets .....	60
9.2.3	Insurance/Warranty Coverage for End-Entities.....	60
9.3	Confidentiality of Business Information .....	61
9.3.1	Scope of Confidential Information .....	61
9.3.2	Information not within the scope of Confidential Information .....	61
9.3.3	Responsibility to Protect Confidential Information.....	61
9.4	Privacy of Personal Information .....	61
9.4.1	Privacy Plan.....	61
9.4.2	Information Treated as Private .....	62
9.4.3	Information not Deemed Private.....	62
9.4.4	Responsibility to Protect Private Information.....	62
9.4.5	Notice and Consent to Use Private Information .....	62
9.4.6	Disclosure Pursuant to Judicial/Administrative Process .....	62
9.4.7	Other Information Disclosure Circumstances.....	62
9.5	Intellectual Property Rights.....	62
9.6	Representations and Warranties .....	62
9.6.1	CA and RA Representations and Warranties.....	62
9.6.2	RA Representations and Warranties .....	63
9.6.3	Subscriber Representations and Warranties.....	64
9.6.4	Relying Parties Representations and Warranties.....	64
9.6.5	Representations and Warranties of Affiliated Organizations.....	64
9.6.6	Representations and Warranties of Other Participants.....	65
9.7	Disclaimers of Warranties.....	65
9.8	Limitations of Liabilities.....	65
9.9	Indemnities .....	65
9.10	Term and Termination .....	65
9.10.1	Term.....	65

9.10.2	Termination .....	65
9.10.3	Effect of Termination and Survival .....	65
9.11	Individual Notices and Communications with Participants .....	65
9.12	Amendments .....	66
9.12.1	Procedure for Amendment .....	66
9.12.2	Notification Mechanism and Period .....	66
9.12.3	Circumstances Under Which OID Must be Changed .....	66
9.13	Dispute Resolution Provisions .....	66
9.14	Governing Law .....	66
9.15	Compliance with Applicable Law .....	66
9.16	Miscellaneous Provisions .....	66
9.16.1	Entire Agreement .....	66
9.16.2	Assignment 66	
9.16.3	Severability 67	
9.16.4	Enforcement (Attorney Fees/Waiver of Rights) .....	67
9.16.5	Force Majeure .....	67
9.17	Other Provisions .....	67

## List of Tables

Table 1	Definitions and Acronyms .....	7
Table 2.	Authentication requirements .....	14
Table 3.	Levels of Assurance for Identity Verification Requirements .....	18
Table 4.	PKI Auditable Events .....	38

---

# SECTION 1 INTRODUCTION

---

## 1.1 OVERVIEW

The Surescripts CA Practice Statement (CPS) describes the practices, such as PKI, used to comply with the Surescripts Certificate Policy (CP), Federal Bridge Certificate Authority (FBCA) Certificate Policy, DirectTrust standards, WebTrust for Certification Authorities, SSL Baseline with Network Security Version 2.1, and identity vetting requirements of NIST 800-63. The CPS 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 CPS supports entities and applications involved in the exchange of electronic messages grounded in the specification of the Direct Project, sponsored by the Office of the National Coordinator (ONC) for Health Information Technology. 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 CPS also supports entities utilizing Transport Layer Security (TLS) and Mutual Authentication TLS (MATLS).

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

This CPS describes the practices under which the Surescripts Certificate Authority operates for two levels of assurance: LoA 2 and 3 (software only). Specifically, this document defines the creation and life-cycle management of X.509 version 3 public key certificates for use in applications supporting Direct message exchange.

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

### 1.1.1 CERTIFICATE POLICY (CP)

Surescripts, L.L.C. ("Surescripts") utilizes a Certificate Policy (CP) to describe its policies for operating a CA. Surescripts has adopted the Direct Trust Community X.509 Certificate Policy (DirectTrust CP), current version 1.2.

Digital certificates that are issued conforming to this CP contain 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 level of assurance at LoA 3 as established by the CP which is available to Relying Parties. A certificate issued by a conforming CA asserts the OID in the certificatePolicies extension.

The Surescripts CA is responsible for all registration authority duties and obligations, including all identification and verification duties related to such applications and the verification of revocation requests. The Surescripts CA utilizes the PKI Repository (as further described in Section 2.1) to publish certain documents and information regarding this CA and its participants. This information is

available only to those entities affiliated with the Surescripts CA; the general public may not have access to this information.

The Surescripts Security Review Committee (SRC) has approved this CPS to define the practices and procedures the Surescripts CA employs when issuing, signing, supporting, and revoking certificates and cryptographic keys.

### 1.1.2 RELATIONSHIP BETWEEN THE SURESCRIPTS CPS AND THE DIRECTTRUST COMMUNITY X.509 CERTIFICATE POLICY

The SRC analyzes the DirectTrust X.509 Certificate Policy and makes a determination of the suitability for cross-certification and the requirement to publish custom requirements.

### 1.1.3 RELATIONSHIP BETWEEN THE SURESCRIPTS CPS AND DIRECTTRUST HISP POLICY

For its HISP services, Surescripts has adopted and complies with DirectTrust HISP Policy version 1.0. Requirements not specifically identified in this CPS may be found in the related DirectTrust Policy.

## 1.2 DOCUMENT NAME AND IDENTIFICATION

This document is the Surescripts Certification Practice Statement (CPS) and was approved for publication by the Surescripts SRC. The CPS corresponds to the policy requirements described in the Surescripts Issuing CA CP, which maps to the DirectTrust Community X.509 Certificate Policy version 1.2.

This CPS defines multiple levels of assurance which are assigned a unique object identifier (OID). The set of policy OIDs are registered under an arc of assigned organizational identifiers as registered in the ISO/ITU OID Registry.

The OID breakdown for Direct Trust is defined as follows:

iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)

The OID Breakdown for Federally Bridged PKI is defined as:

joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) pki(2) cert-policy(1) fpki-common(3)

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
id-fbpki-common arc		2.16.840.1.101.3.2.1
id-fbpki-common-policy	LoA 3	2.16.840.1.101.3.2.1.3.6
id-fbpki-common-hardware	LoA 3	2.16.840.1.101.3.2.1.3.7
id-fbpki-common-authentication	LoA 3	2.16.840.1.101.3.2.1.3.13
Surescripts PKI		1.3.6.1.4.1.37583
Surescripts Low Assurance Policy		1.3.6.1.4.1.37583.509.50.1.1
Surescripts Basic Assurance Policy		1.3.6.1.4.1.37583.509.50.1.2
Surescripts Medium Assurance Policy		1.3.6.1.4.1.37583.509.50.1.3

Certificates issued under DirectTrust policies by this CA are performed at levels of assurance or conform to the requirements for a given healthcare entity category (Cat) at the appropriate OID or OIDs, as defined above in the Certificate Policies X.509v3 standard extension. See sections 3.2.2 and 3.2.3.1 for details of each LoA and Cat.

Certificates used for TLS or MATLS conform to the WebTrust for Certification Authorities, SSL Baseline with Network Security Version 2.1 and are identified by the OID's for Surescripts PKI policies.

This CPS completely applies to any entity asserting one or more of the Surescripts OIDs identified above with the exception of SS-TLS. Unique differences for Surescripts PKI policy certificates are identified in their respective sections. All other OIDs mentioned herein belong to their respective owners. Subsequent revisions to this CPS might contain additional OID assignments than those identified above.

## 1.3 PKI PARTICIPANTS

The following roles are applicable in the administration and operation of the Surescripts PKI:

## 1.3.1 PKI AUTHORITIES

### 1.3.1.1 PKI POLICY AUTHORITY

The Surescripts PKI Policy Authority (SSPA) is the governing body for this Certificate Authority. The SSPA is comprised of the Chief Information Security Officer, security, and Product Innovation teams. The SSPA is responsible for:

- Overseeing the creation and updates for Certificate Policies (CP) and Certification Practice Statements (CPS) and plans for implementing any accepted changes.
- Providing timely and responsive coordination to approved Business Organizations and their Sponsors.
- Reviewing the CPS to ensure its continuous conformance to the stipulations of the CP.
- Reviewing the results of any CA compliance audits to determine if the CA is adequately meeting the stipulations of the CP and associated approved CPS documents, and make recommendations to the CA regarding corrective actions, or other measures that might be appropriate, such as revocation of CA certificates or changes to the CP or CPS.
- Perform decisions on (i) policy and technical & business practices and issues related to Surescripts Certification Authorities (CA); (ii) approval of cross-certification with the applicable Bridge CA; (iii) approval of the issuance of CA certificates from the Surescripts Root CA.

Decisions by the SSPA apply to the issuance of cross-certificates and CA certificates. The SSPA does not prescribe how entities are to rely on digital certificates for transactions. All entities are free to accept or reject any digital certificate issued by any other entity at their sole discretion. The SSPA reports to the Security Review Committee for ultimate approval for its activities and formal adoption of recommended changes in procedure and this CPS.

## 1.3.2 CERTIFICATION AUTHORITIES

### 1.3.2.1 Root CA

The Surescripts Root CA is a trust anchor for certificate holders of a PKI domain when the certificate holders act as the relying party. The Surescripts Root CA issues a CA signing certificate to the Surescripts CA. Additionally, the Surescripts Root CA issues signing certificates to multiple CAs.

The Surescripts Root CA creates, signs, and issues public key certificates to Surescripts Subordinate CAs to issue certificate holder certificates.

The Surescripts Root CA is the trust anchor for relying parties.

### 1.3.2.2 DIRECT CA

The Surescripts Direct CA is a Subordinate Issuing CA whose primary function is to issue certificates to the end entities for Direct messaging exchange. It does not issue certificates to other CAs with the exception of the cross-certificate to the DirectTrust Root CA.

### 1.3.2.3 CROSS CERTIFIED CA

A Cross-Certified CA is an organization that is operating a CA that has cross-certified with Surescripts through the Surescripts Direct CA. The DirectTrust CA is an example of a CA which has cross-certified with the Surescripts Direct CA.

#### **1.3.2.4 ISSUING CA**

The Surescripts Issuing CA is a Subordinate Issuing CA whose primary function is to issue certificates to the end entities for server and client authentication.

### **1.3.3 REGISTRATION AUTHORITIES**

The Surescripts Registration Authority (RA) is a combination of people and system processes that operates an identity management system (IdMS) and collects and verifies Subscriber information. The RA collects and verifies identity information from Surescripts Subscribers using procedures that implement the identity validation policies set forth in this document. The Surescripts Registration Authority (RA) will exist as the only accredited RA for the Surescripts Certification Authority.

### **1.3.4 SUBSCRIBERS, SUBJECTS AND APPLICANTS**

A Surescripts Direct Subscriber is an entity who uses Direct services and PKI to support Direct transactions and communications. Subscribers are not the party identified in a certificate 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 Surescripts CA for the certificate's issuance in accordance with this CPS. 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 abides by the required Subscriber Agreements. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

### **1.3.5 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 holds and manages PKI private keys associated with a Direct digital certificate on behalf of the Subscriber.

### **1.3.6 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).

### **1.3.7 OPERATIONAL AUTHORITY (OA)**

The Surescripts Operational Authority is the organization that operates and maintains the Surescripts Certificate Servers, including issuing certificates, posting those certificates and Certificate Revocation Lists (CRLs) into the Surescripts PKI Repository, and ensuring the continued availability of the repository to all users. The OA acts upon approval of the SRC.

### **1.3.8 OTHER PARTICIPANTS**

No stipulation.

## **1.4 CERTIFICATE USAGE**

### **1.4.1 APPROPRIATE CERTIFICATE USES**

The primary use for a Direct X.509 certificate, asserting a policy identifier other than the ss-tls policy, 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 CPS are only used for the purposes designated in the key usage and extended key usage fields found in the certificate.

The primary use of certificate that asserts the ss-tls policy is the establishment and encryption of sessions employing TLS or MATLS communication.

However, each Relying Party must evaluate the application environment and associated risks before deciding on whether to accept a certificate issued by this CA 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 stated level of assurance when the certificate was issued. Certificates issued under this Certification Practice Statement may not be used where prohibited by law.

Except as allowed in Section 1.4.1 above, all other uses of Certificates are prohibited. Without limiting the foregoing, Subscribers will not: (i) use Certificates on behalf of any other entity; (ii) sell or otherwise transfer the Certificate; (iii) copy, enhance, modify or decompile the Certificate (except as allowed by applicable law; or (iv) perform any public or private key operations with the Certificate or associated public key or private key with a name other than that in the Subject field in the Certificate.)

## **1.5 POLICY ADMINISTRATION**

### **1.5.1 ORGANIZATION ADMINISTERING THE DOCUMENT**

The Surescripts Security Review Committee (SRC) is responsible for this CPS.

The Surescripts SRC includes members of the Surescripts Information Security group, Systems Engineers, and their management.

The Surescripts SRC may amend this Certification Practice Statement, or any part thereof, at any time, at its discretion. Prior to any amendment of this CPS, the Surescripts SRC will provide notice of



any proposed change in writing to all CAs that are directly cross-certified with its CAs, and may specify a review period in any such notice.

## 1.5.2 CONTACT PERSON

Questions regarding this CPS are to be directed to:

Certificate Policy Manager  
Surescripts LLC  
920 Second Avenue South  
Minneapolis, MN 55402

Inquiries may be forwarded to [certificate.services@Surescripts.com](mailto:certificate.services@Surescripts.com).

## 1.5.3 PERSON DETERMINING CPS SUITABILITY FOR THE CERTIFICATE POLICY

The Surescripts SRC, security staff, and peers will ensure compliance between this CPS and the CP. Third party services may be used to attest to this compliance.

## 1.5.4 CERTIFICATION PRACTICE STATEMENT APPROVAL PROCEDURES

The Surescripts CA submits this CPS to a compliance analysis and audit against each applicable CP as described in Section 8 of this CPS. The CA's CPS shall be required to meet all facets of its policy. The CA may not declare conformance with this CPS until the compliance analysis and audit is complete and all discrepancies resolved.

When a change to this CPS is required, the Surescripts Certificate Policy Manager will request a meeting with the Surescripts SRC for revision approval.

## 1.6 DEFINITIONS AND ACRONYMS

**Table 1 Definitions and Acronyms**

Term	Definition
Authentication	The process of establishing that individuals, organizations or things are who or what they claim to be.
CA	Certification Authority
CCB	Change Control Board (In this document, the term refers to the Surescripts Security Operations CCB.)
CP	Certificate Policy: a named set of rules that indicate the applicability of a certificate to a particular community and/or class of application with common security requirements
CPS	Certification Practice Statement
CRL	See Certificate Revocation List

Term	Definition
CSR	Certificate Signing Request
Certificate	Data structure that: 1) identifies the Certification Authority issuing it; 2) names or otherwise identifies its Subject and Subscriber; 3) contains a Public Key that corresponds to a Private Key under the control of the Subscriber; 4) identifies its period of validity; and (5) contains a certificate serial number and is digitally signed by the CA issuing it.
Certificate Class	All the certificates issued under a particular named Certificate Policy.
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 Revocation List (CRL)	A list maintained by a Certification Authority of the certificates that it has issued which are revoked prior to their stated expiration date.
Certificate Signing Request (CRL)	A special data structure containing all the information necessary to request a digital certificate from a certification authority. Per the PKCS10 v1.7 standard: "A certification request consists of a distinguished name, a public key, and optionally a set of attributes, collectively signed by the entity requesting certification. Certification requests are sent to a certification authority, which transforms the request into an X.509 public-key certificate."
Certification Authority (CA)	Entity that authorizes and issues a certificate. The CA: 1) identifies and authenticates the intended Subject to be named in the Certificate; 2) verifies that certain Subscribers possess the Private Key that corresponds to the Public Key that will be listed in the Certificate 3) creates and digitally signs the Certificate. For this Surescripts CA CPS, the Surescripts CA is the body responsible for generating and certifying the Public Key Certificates for the Surescripts business.
Certification Practice Statement (CPS)	Document that specifies practices a CA employs in issuing and revoking certificates.
Confirm	To ascertain through appropriate inquiry and investigation.
DN	Distinguished Name
IA5String	ASN.1 notation representing a free text value
ID	Identity
IETF	Internet Engineering Task Force  A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
ISSO	Information Systems Security Officer  An individual responsible for establishing and maintaining the Systems Security enterprise vision, strategy and program as it relates to ensuring that Information assets are adequately protected.
LoA	Level of Assurance

Term	Definition
Non-production	Describes a system, environment, subscriber, or relying party that does not interact or participate in a Surescripts business' Production environment.
Object Identifier	The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. A number that identifies an object's position in a global object registration tree.
OCSP	Online Certificate Status Protocol
OID	Object Identifier
Participants	An individual or organization that plays a role within the PKI for the Surescripts business as a subscriber, relying party, CA, RA, certificate manufacturing authority, repository service provider, or similar entity.
Pass Phrase	A string of words and characters (usually 20 characters or more) that a user types into a computer to confirm his or her identity. A more secure form of a password or PIN.
PIN	Personal Identification Number that the Subscriber selects and uses to import the Private Key into its own software package.
PKI	See Public Key Infrastructure.
PKI Repository	A networked electronic information resource, available to Surescripts PKI Subscribers and Relying Parties, to which CA Certificates, CRLs, PKI policies, and related information can be published.
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.
RA	See Registration Authority.
Registration Authority (RA)	Entity responsible for identification and authentication of certificate subjects. Component of a Surescripts CA that provides the user interface and business logic for issuing and administering user certificates.
Relying Party	Person who has received a Certificate and a digital signature verifiable with reference to a Public Key listed in the certificate, and who is in a position to rely on them.
Repository	Trustworthy system for storing and retrieving Certificates or other information relevant to Certificates.
Revoke a Certificate	Permanently end the operational period of a certificate from a specified time forward.
RFC	Request For Comments
Root CA	Top-level Certification Authority in a trust hierarchy.

Term	Definition
S/MIME	Secure Multipurpose Internet Mail Extensions
SRC	Security Review Committee
SSL Baseline Requirements	CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.1
Subject	The person or device that is the subject of a Certificate.
Subordinate CA	Lower-level Certification Authority in a trust hierarchy. Subordinate CA certificates are signed by the Root CA and are checked for authenticity against the Root CA.
Subscriber	<p>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.</p> <p>A Subscriber is the person or entity being issued Private Keys and/or Certificates under terms of this Surescripts CA CPS.</p>
Surescripts CA	Body responsible for generating and certifying the Public Key certificates for the Surescripts Direct business.
Surescripts PKI	The PKI developed for the Surescripts Direct business.
Surescripts Security Operations	Surescripts Security Operations is the organizational unit responsible for developing and maintaining the Certification Authority and other Surescripts PKI entities.
Surescripts Security Operations CCB	The Surescripts Security Operations Change Control Board (CCB) is the organizational unit responsible for ensuring Surescripts Security Operations develops the PKI according to requirements
Trustworthy System	<p>Computer hardware, software, and procedures that:</p> <ol style="list-style-type: none"> <li>1) are reasonably secure from intrusion and misuse;</li> <li>2) provide a reasonably reliable level of availability, reliability, and correct operation;</li> <li>3) are reasonably suited in performing their intended functions;</li> <li>4) adhere to generally accepted security principles.</li> </ol>
URI	Universal Resource Identifier

---

## SECTION 2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

---

### 2.1 REPOSITORIES

The Surescripts CAs and RAs operate repositories in support of operations required by this CPS and the CP. The CA ensures that its root certificate and the revocation data for issued certificates are available through an externally-facing repository.

#### 2.1.1 REPOSITORY OBLIGATIONS

The repositories holding certificate status data are operated 24 hours a day, 7 days a week within an active cluster with a high availability expectation to exceed 99% availability overall per year .

### 2.2 PUBLICATION OF CERTIFICATION INFORMATION

#### 2.2.1 PUBLICATION OF CERTIFICATES AND CERTIFICATE STATUS

The Surescripts CA maintains a Certificate Revocation List (CRL) and exposes its location in the CRL Distribution Points X.509v3 extension. The Surescripts CA maintains an equivalent Online Certificate Status Protocol (OCSP) Responder and expose its location in the Authority Information Access X.509 extension. This is done in accordance with the relevant Sections within 4.9 and 7.3.

CA and End Entity certificates contain valid Uniform Resource Identifiers (URIs) that are accessible by Relying Parties. The CA publishes its CA certificate and any other intermediate or trust anchor certificates necessary to validate the Surescripts CA.

The publicly accessible directory system shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

The certificate status server (CSS) shall be designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

#### 2.2.2 PUBLICATION OF CA INFORMATION

The Surescripts CA freely publishes its Surescripts CA Certificate Policy and information concerning the CA necessary to support its operation and use. Information on how to obtain a copy of its CPS shall be provided to any party with legitimate interest.

### **2.2.3 INTEROPERABILITY**

No stipulation.

## **2.3 FREQUENCY OF PUBLICATION**

The Surescripts Certificate Policy (CP), and any ensuing changes, shall be made publicly available within 14 days of approval through the Surescripts consensus process.

This Surescripts Certification Practice Statement (CPS) is considered proprietary and confidential to Surescripts and will be published internally and available only to parties with a contractual need to know.

CRLs expire every 7 days or less and must be updated immediately when a new entry is added to it, or every 7 days, whichever is earlier.

## **2.4 ACCESS CONTROLS ON REPOSITORIES**

The Surescripts CA and RA protect repository information not intended for public dissemination or modification. The Surescripts CA provides unrestricted read access to its repositories for legitimate uses and has implemented logical and physical controls to prevent unauthorized write access to such repositories.

The Surescripts CA and RA repository is instantiated within the Microsoft Active Directory Certificate Services platform. This repository can only be modified by the Surescripts CA application or the Surescripts SRC or authorized representatives.

## SECTION 3 IDENTIFICATION AND AUTHENTICATION

---

### 3.1 NAMING

#### 3.1.1 TYPES OF NAMES

All Organizational certificates use non-null and unique DN name forms for the Issuer and Subject names. As specified in the published document “Direct Project Applicability Statement for Secure Health Transport”, certificates tied to full Direct addresses (“Address certificates”) contain the Direct address in the subjectAltName extended attribute as an rfc822Name. Certificates tied to a Direct domain (“Organizational certificates”) contain the domain name in two places:

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

The subjectAltName extension and Subject Common Name (CN) field may not contain reserved IPs or internal server names. Any existing certificates with such extension or field settings will be revoked by October 2016.

#### 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 are easily understood by humans.

#### 3.1.3 ANONYMITY OR PSEUDONYMITY OF SUBSCRIBERS

This CA does not issue anonymous certificates. Pseudonymous certificates are issued when the name space uniqueness requirements are met.

#### 3.1.4 RULES FOR INTERPRETING VARIOUS NAME FORMS

No stipulation.

#### 3.1.5 UNIQUENESS OF NAMES

The OA enforces name uniqueness of the certificate subject DN within the CA's X.500 namespace.

### 3.1.6 RECOGNITION, AUTHENTICATION, AND ROLE OF TRADEMARKS

Subscribers cannot request certificates with any content that infringes the intellectual property rights of another entity. This CA will reject any application or require revocation of any certificate that is part of a trademark dispute.

This CA will implement a process to prevent any certificate attributes from including a name, DBA (doing business as), trade name, trademark, address, location, or other text that refers to a specific or natural person or Legal Entity unless the CA has verified this information in accordance with the SSL Baseline Requirements Section 11.2 and the certificate also contains subject:organizationName, subject:localityName, and subject:countryName attributes, also verified in accordance with SSL Baseline Requirements Section 11.2.

## 3.2 INITIAL IDENTITY VALIDATION

### 3.2.1 METHOD TO PROVE POSSESSION OF PRIVATE KEY

All CSRs provided by subscribers must be signed by the private key for which the certificate is to be issued.

In cases when the private key is generated by the RA; no additional proof of private key possession is required.

### 3.2.2 AUTHENTICATION OF ORGANIZATION IDENTITY

**Table 2. Authentication requirements**

Certificate	Validation
Organizational Certificates for Direct Messaging	<p>Requests for organizational certificates for Direct messaging include the organization name, mailing address, and a Clinical Interoperability Agreement that verifies 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).</p> <p>The requesting organizations are qualified in one of the following categories:</p> <ul style="list-style-type: none"> <li>• HIPAA Covered Entity.</li> <li>• HIPAA Business Associate, or</li> </ul> <p>The RA verifies the applicant organization's healthcare category in accordance with the process established in this CPS that meets the following minimum requirements:</p>



	Category requirements for Healthcare Organizations
DT.org CE	Applicant represents that it is a Covered Entity as defined in HIPAA.
DT.org BA	<p>Applicant represents that it will limit its use of any Digital Certificate issued to it pursuant to its CP for purposes required in its capacity as a Business Associate (BA), as defined in HIPAA.</p> <p>The RA will confirm that such representation has been made in an appropriate legally binding agreement.</p> <p>Relying Parties may be required by government statute or regulations to have additional agreements in place with the BA.</p>
	The RA also verifies 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 Surescripts CA obtains authoritative 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.
	<b>NOTE:</b> Certificates asserting an organizational affiliation may also assert the OID corresponding to that organization's healthcare category.
Certificate	<b>Validation</b>
Surescripts TLS Certificates	<p>If the Applicant requests a Certificate that will contain Subject Identity Information comprised only of the countryName field, then the CA SHALL verify the country associated with the Subject using a verification process meeting the requirements of SSL Baseline Requirements 11.2.5 and If the Applicant requests a Certificate that will contain the countryName field and other Subject Identity Information, then the CA SHALL verify the identity of the Applicant, and the authenticity of the Applicant Representative's certificate request using a verification process meeting the requirements of this section and that is described in the CA's Certificate Policy and/or Certification Practice Statement in section 3.2.</p> <p>The CA SHALL inspect any document relied upon under this section for alteration or falsification.</p>
	<p>Subject Identity</p> <p>If the Subject Identity Information is to include the name or address of an organization, the CA SHALL verify the identity and address of the organization and that the address is the Applicant's address of existence or operation. The CA SHALL verify the identity and address of the Applicant using documentation provided by, or through communication with, at least one of the following:</p> <ol style="list-style-type: none"> <li>1. A government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;</li> <li>2. A third party database that is periodically updated and considered a Reliable Data Source;</li> </ol>

	<p>3. A site visit by the CA or a third party who is acting as an agent for the CA; or</p> <p>4. An Attestation Letter.</p> <p>The CA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address. Alternatively, the CA MAY verify the address of the Applicant (but not the identity of the Applicant) using a utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable</p>
	<p>DBA/Tradename</p> <p>If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following:</p> <ol style="list-style-type: none"> <li>1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;</li> <li>2. A Reliable Data Source;</li> <li>3. Communication with a government agency responsible for the management of such DBAs or tradenames;</li> <li>4. An Attestation Letter accompanied by documentary support; or</li> <li>5. A utility bill, bank statement, credit card statement, government-issued tax document, or other form of identification that the CA determines to be reliable.</li> </ol>
	<p>Individual Applicant</p> <p>If an Applicant is a natural person, then the CA SHALL verify the Applicant's name, Applicant's address, and the authenticity of the certificate request. The CA SHALL verify the Applicant's name using a legible copy, which discernibly shows the Applicant's face, of at least one currently valid government-issued photo ID (passport, drivers license, military ID, national ID, or equivalent document type). The CA SHALL inspect the copy for any indication of alteration or falsification. The CA SHALL verify the Applicant's address using a form of identification that the CA determines to be reliable, such as a government ID, utility bill, or bank or credit card statement. The CA MAY rely on the same government issued ID that was used to verify the Applicant's name. The CA SHALL verify the certificate request with the Applicant using a Reliable Method of Communication.</p>
	<p>Country</p> <p>If the subject:countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following:</p> <ol style="list-style-type: none"> <li>(a) the IP Address range assignment by country for either (i) the web site's IP address, as indicated by the DNS record for the web site or (ii) the Applicant's IP address;</li> <li>(b) the ccTLD of the requested Domain Name;</li> <li>(c) information provided by the Domain Name Registrar; or</li> <li>(d) a method identified in Section SSL Baseline Requirements 11.2.1.</li> </ol> <p>The CA SHOULD implement a process to screen proxy servers in order to prevent reliance upon IP addresses assigned in countries other than where the Applicant is actually located.</p>

### **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 Direct 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 identity of an individual requesting a Direct Address certificate.

The RA verifies an individual's identity in accordance with the process established below:

**Table 3. Levels of Assurance for Identity Verification Requirements**

<p><b>DT.org LoA 2</b> (Equivalent to NIST 800-63 Level 2 or Kantara Level 2 or FBCA Basic)</p>	<p>Applicant supplies his or her full legal name, an address of record, and date of birth.</p> <p><b>For In-Person vetting:</b> the applicant also provides valid government issued photo ID.</p> <p><b>RA</b> inspects photo - ID; compares picture to Applicant; and records the ID number, address and date of birth (DoB).</p> <p><b>CA</b> 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.</p> <p><b>For Remote vetting:</b> 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.</p> <p><b>RA</b> 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).</p> <p><b>CA</b> 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.</p> <p>Any of the identity verification methods listed for a higher level is also acceptable.</p>
---	---

<p><b>DT.org LoA 3</b> (Equivalent to NIST 800-63 Level 3 or Kantara Level 3 or FBCA Medium)</p>	<p>Applicant supplies his or her full legal name, an address of record, and date of birth.</p> <p><b>For In-Person vetting:</b> the applicant also provides valid government issued photo ID.</p> <p><b>RA</b> 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.</p> <p><b>CA</b> 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.</p> <p><b>For Remote vetting:</b> the applicant provides valid government issued Photo ID identifier + a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID and account.</p> <p><b>RA</b> 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).</p> <p><b>CA</b> 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.</p> <p>Any of the identity verification methods listed for a higher level is also acceptable.</p>
--	--

Additionally, the RA shall record the process that was followed for issuance of each certificate. The process documentation and authentication requirements shall include the following:

- The identity of the person performing the identification;
- A signed declaration by that person that he or she verified the identity of the Applicant as required by the CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury);
- Unique identifying number(s) from the ID(s) of the applicant, or a facsimile of the ID(s);
- The biometric of the applicant;
- The date and time of the verification; and
- A declaration of identity signed by the applicant using a handwritten signature and performed in the presence of the person performing the identity authentication, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury).

If the requested Surescripts Direct digital certificate is to be used by a patient or on behalf of a patient, the RA verifies the patient identity with the process established at Section below:

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

### 3.2.3.2 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 Direct digital 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, the RA also records 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 are performed:

- The HISP Information Systems Security Officer or equivalent is 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 does not imply that the subject is a single individual,
- The list of those holding the shared private key is provided to, and retained by, the Surescripts Operational Authority or its designated representative.

### 3.2.3.3 AUTHENTICATION OF HUMAN SUBSCRIBERS FOR ROLE-BASED CERTIFICATES

No stipulation.

### 3.2.3.4 AUTHENTICATION OF DEVICES

Not being used at the present time.

## 3.2.4 NON-VERIFIED SUBSCRIBER INFORMATION

All Subscriber information placed in a Surescripts CA certificate uses pre-completed templates and is verified by the RA within the application process. All certificates are issued within 30 days of completion of verification.

### **3.2.5 VALIDATION OF AUTHORITY**

The Surescripts RA verifies the association between an organization requesting an organizational certificate and the individual representing the organization during the identity verification processes described in section 3.2.3.

### **3.2.6 CRITERIA FOR INTEROPERATION**

To be deemed a conforming Surescripts Issuing CA, the CA issues certificates according to the Surescripts Certificate Policy.

## **3.3 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS**

### **3.3.1 IDENTIFICATION AND AUTHENTICATION FOR ROUTINE RE-KEY**

A subscriber's identity may be established through use of current signature key, except that identity shall be re-established through the original registration process requirements at least once every nine years from the time of initial registration. CA certificate re-key shall follow the same procedures as initial certificate issuance.

### **3.3.2 IDENTIFICATION AND AUTHENTICATION FOR RE-KEY AFTER REVOCATION**

If a Surescripts certificate is revoked, the Subscriber goes through the initial identity verification process described in section 3.2 to obtain a new certificate.

## **3.4 IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST**

All revocation requests are 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. Revocation requestors are indisputably identified and authenticated as the responsible party of the subscriber organization. Other requestors must manage their case for a revocation working with their Surescripts support liaison.





### **4.2.3 TIME TO PROCESS CERTIFICATION APPLICATIONS**

All Subscriber information placed in a Surescripts certificate is verified and a certificate issued within 30 days of completion of verification.

### **4.2.4 REVIEW OF CAA RECORDS**

Surescripts does not review CAA records as part of the certificate approval process. DNS entries for FQDN's are verified through registered internet domain record sources as appropriate.

## **4.3 ISSUANCE**

### **4.3.1 CA ACTIONS DURING CERTIFICATE ISSUANCE**

The Surescripts CA ensures that the public key is bound to the correct Subscriber and generates the certificate. The Surescripts CA publishes the certificate as specified in section 4.4.2. The Surescripts CA performs all its actions during the certificate issuance process within a perimeter-protected network using encrypted transmissions.

### **4.3.2 NOTIFICATION TO SUBSCRIBER OF CERTIFICATE ISSUANCE**

The Subscriber is notified via e-mail that his certificate has been issued.

## **4.4 CERTIFICATE ACCEPTANCE**

### **4.4.1 CONDUCT CONSTITUTING CERTIFICATE ACCEPTANCE**

All Subscribers are required to sign a Subscriber Agreement Form which stipulates the terms of certificate acceptance and use. The signing of this form and the use of the credential is considered certificate acceptance.

### **4.4.2 PUBLICATION OF THE CERTIFICATE BY THE CA**

The Surescripts CA makes its certificates available to the public using Microsoft's Lightweight Directory Access Protocol (LDAP).

### **4.4.3 NOTIFICATION OF CERTIFICATE ISSUANCE BY THE CA TO OTHER ENTITIES**

No stipulation.

## **4.5 KEY PAIR AND CERTIFICATE USAGE**

### **4.5.1 SUBSCRIBER PRIVATE KEY AND CERTIFICATE USAGE**

All Subscribers are required to sign a Subscriber Agreement Form which stipulates the terms of certificate acceptance and private use, including, protect it from access by unauthorized parties and 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**

Surescripts certificates conform to the policies provided by the Surescripts Certificate Policy. Relying parties should review this document and understand those policies. The Surescripts CA publishes a certificate revocation list (CRL) and maintains an OCSP Responder. Relying parties need to 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 is not allowed at this time

### **4.6.1 CIRCUMSTANCE FOR CERTIFICATE RENEWAL**

Certificate renewal is not allowed at this time

### **4.6.2 WHO MAY REQUEST RENEWAL**

Certificate renewal is not allowed at this time

### **4.6.3 PROCESSING CERTIFICATE RENEWAL REQUESTS**

Certificate renewal is not allowed at this time

### **4.6.4 NOTIFICATION OF NEW CERTIFICATE ISSUANCE TO SUBSCRIBER**

Notification of Certificate issuance follows the manual process defined in Section 4.3.2

### **4.6.5 CONDUCT CONSTITUTING ACCEPTANCE OF A RENEWAL CERTIFICATE**

Certificate renewal is not allowed at this time

#### **4.6.6 PUBLICATION OF THE RENEWAL CERTIFICATE BY THE CA**

Certificate renewal is not allowed at this time

#### **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 will be assigned a different validity period, key identifiers, specify a different CRL distributionPoint or OSCP 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 is not be revoked, but is not further re-keyed, renewed, or modified.

#### **4.7.1 CIRCUMSTANCE FOR CERTIFICATE RE-KEY**

A certificate is re-keyed before it's the end of its validity period and when no other information besides its keys and validity period are changing. A revoked certificate is not re-keyed.

#### **4.7.2 WHO MAY REQUEST CERTIFICATION OF A NEW PUBLIC KEY**

A Surescripts 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 Surescripts RA approves or rejects Subscriber certificate re-keying requests. Identity verification of the Subscriber is 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 is not allowed at this time.

**4.8.1 CIRCUMSTANCE FOR CERTIFICATE MODIFICATION**

Certificate modification is not allowed at this time

**4.8.2 WHO MAY REQUEST CERTIFICATE MODIFICATION**

Certificate modification is not allowed at this time

**4.8.3 PROCESSING CERTIFICATE MODIFICATION REQUESTS**

Certificate modification is not allowed at this time

**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..0000.

**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 is 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, or
- 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 is revoked, placed on the certificate revocation list (CRL) and has its revoked status reflected in OCSP responses.

### 4.9.2 WHO CAN REQUEST REVOCATION

The RA or OA may request revocation of a certificate, or it 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 identifies the certificate to be revoked by serial number and explains the reason for revocation. A Surescripts 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 Surescripts 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.

FPKIPA and other non-customers may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report". Submit these to [certificate.services@surescripts.com](mailto:certificate.services@surescripts.com). Surescripts customers should follow the appropriate support procedure or open a self-service support ticket at [surescripts.com](https://surescripts.com).

### 4.9.4 REVOCATION REQUEST GRACE PERIOD

There is no grace period for revocation under this CPS. Subscribers and authorized PKI entities 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**

Surescripts will revoke certificates as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

#### **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**

The Surescripts CA CRL is issued and posted to the repository listed in section 2.2.1 every 7 days even when there are no changes or updates to be made to ensure timeliness of information. A CRL may be issued more frequently than every 7 days if new entries are made to the CRL. The Surescripts CA ensures that superseded CRLs are removed from the public repository upon posting of the latest CRL.

Certificates will be revoked as quickly as practical upon receipt of a proper revocation request. Revocation requests shall be processed before the next CRL is published. Exceptioning those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance shall be processed before the following CRL is published.

#### **4.9.8 MAXIMUM LATENCY OF CRLS**

CRLs are posted upon generation but within no more than four hours after generation. Furthermore, a new CRL is 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**

The Surescripts CA deploys an Online Certificate Status Protocol (OCSP) responder. Status information must be updated and available to relying parties within 18 hours of certificate revocation.

#### **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**

The Surescripts CA does not support suspended certificates.

#### **4.9.14 WHO CAN REQUEST 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**

#### **4.10.1 OPERATIONAL CHARACTERISTICS**

The status of public certificates is available via a CRL or OCSP responder. These services are included in an high availability (HA) cluster where responders are available concurrently in multiple data center locations.

#### **4.10.2 SERVICE AVAILABILITY**

Certificate Status Services are available 24 X 7 without scheduled interruption.

#### **4.10.3 OPTIONAL FEATURES**

OCSP is an optional status service that is available.

### **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 Surescripts 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.



## SECTION 5 **FACILITY MANAGEMENT AND OPERATIONS CONTROLS**

---

### **5.1 PHYSICAL CONTROLS**

Surescripts has implemented commercially sound, security controls in order to protect its CA from environmental, physical and other threats.

#### **5.1.1 SITE LOCATION AND CONSTRUCTION**

The Surescripts CA components are housed within a commercially contracted data center grade environment that deters, prevents and detects unauthorized use of, access to, or disclosure of sensitive information and systems.

#### **5.1.2 PHYSICAL ACCESS**

Access to the Surescripts data center is restricted by magnetic key card and biometric readers. Entry is restricted to OA personnel only

The Surescripts CA private keys are protected by FIPS 140-2 level 3 Hardware Security Modules.

#### **5.1.3 POWER AND AIR CONDITIONING**

The Surescripts CA utilizes the same power and cooling protection as other Surescripts critical systems. This includes:

- power systems to ensure continuous, uninterrupted access to electric power, sufficient for a minimum of 6 hours operation in the absence of commercial power, and
- heating and air conditioning systems to control temperature and relative humidity

#### **5.1.4 WATER EXPOSURES**

The Surescripts CA has systems in place to minimize the impact of water exposure on any Surescripts CA component. The same safeguards protect other Surescripts critical systems.

## **5.1.5 FIRE PREVENTION AND PROTECTION**

The Surescripts CA is protected by systems designed to prevent and extinguish fires and/or prevent damage from exposure to flame or smoke. These systems have been designed to comply with local fire safety regulations.

## **5.1.6 MEDIA STORAGE**

All media containing production data or software related to the Surescripts CA is housed within Surescripts facilities or in secure off-site storage facilities with appropriate physical and logical controls designed to limit access to unauthorized personnel and to provide protection against accidental damage.

Media located within the Surescripts campus is controlled by the Surescripts Security Operations team.

## **5.1.7 WASTE DISPOSAL**

Any media containing unencrypted critical data is disposed of by erasure or destruction, as specified in the DoD National Industrial Security Program Operating Manual (NISPOM).

## **5.1.8 OFF-SITE BACKUP**

The Surescripts CA routinely performs backups of critical system data, audit log data, and other sensitive information. Backup procedures are addressed within Security Operations Production Support Plan.

# **5.2 PROCEDURAL CONTROLS**

## **5.2.1 TRUSTED ROLES**

### **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.

- Administrators for the Surescripts CA Hardware Security Modules (HSMs) are:
  - Surescripts HSM Partition Owner (Black Key): One of a group of individuals who must act in concert to control the security of HSM.
  - Surescripts HSM Domain Owner (Red Key): One of a group of individuals who may act in concert to control HSM domain activity.
  - Surescripts HSM Administrator (Blue Key): One of a group of individuals who may act individually to control the routine operation of the HSM.
  - Surescripts CA Environment Gatekeeper: One of a group of individuals who must act in concert to gain physical access to the Surescripts CA computer system environment.

Other Administrators for the Surescripts CA include:

- Surescripts CA System Administrator: Technical management of operating system.
- Surescripts CA Security Administrator: Technical management of the Surescripts CA, using the system console, software installation and configuration, and the HSM.

#### **5.2.1.2 OFFICER**

The Surescripts CA Vetter manages daily activities related to registration authority duties; for example, reviews and approves or denies Certificate applications and Certificate revocation requests.

#### **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 CPS.

#### **5.2.1.4 OPERATOR**

The CA 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**

- Physical Access and one (1) Surescripts CA System Administrator are required to gain privileged access (Privileged System Access) to the Surescripts CA system(s).

- Physical Access and one (1) Surescripts CA System Administrator for registration authority duties are, required for Privileged System Access to the Surescripts CA system(s) for registration authority duties.
- Physical Access, Privileged System Access and two (2) individuals from the “Surescripts HSM Administrator Key Holder” group are required to perform administrative functions with the HSM. Administrative functions include replacing lost or damaged keys or re-initializing an HSM.
- Physical Access, Privileged System Access, and two (2) individuals from the “Surescripts HSM Partition Owner” group are required to perform operator functions with the HSM.
- Physical Access, an authorized Surescripts CA Operator Certificate, and one (1) individual are required for operational management of the Surescripts CA using the web-based GUI.
- Physical Access, an authorized Surescripts CA Operator for registration authority duties Certificate, and one (1) individual are required for operational management of registration authority duties using the web-based GUI. For example, requires Surescripts CA Vettors for registration authority duties, other Surescripts CA Operators for registration authority duties, and Surescripts CA auditors for registration authority duties.
- One individual with an authorized Surescripts CA vetting Certificate for registration authority duties is required to perform the tasks in the role of Surescripts CA Vetter for registration authority duties.
- One individual from Surescripts Security Operations with an authorized Surescripts CA auditing Certificate for registration authority duties is required to perform the tasks in the role of Surescripts CA Auditor for registration authority duties.
- Physical Access and one (1) Surescripts CA network administrator are required to administer network hardware.
- One (1) Surescripts CA network administrator required to perform Surescripts CA firewall administration.

### **5.2.3 IDENTIFICATION AND AUTHENTICATION FOR EACH ROLE**

- Surescripts HSM Administrator Key Holder: Possesses a physical, unique token with a pass phrase associated with that token. That token will be from the Administrative Key Set created during HSM initialization.
- Surescripts HSM Operator Key Holder: Possesses a physical, unique token with a pass phrase associated with that token. The token will be from the Operator Key Set(s) created during HSM initialization.

- Surescripts CA Environment Gatekeeper: Possesses a physical and unique token with associated PIN, which is verified by the physical system rack protecting the environment.
- Surescripts CA Manager: Identified as an individual in a position of authority over daily activities in the Surescripts CA environment.
- Surescripts CA System Administrator: Requires Physical Access and is identified and authenticated by the System Access Control in place on the Surescripts CA system.
- Surescripts CA Security Administrator: Requires Physical Access and is identified and authenticated by the System Access Control in place on the Surescripts CA System.
- Surescripts CA Operator: Requires Physical Access and is identified and authenticated by the System Access Control in place on an Administrative workstation. They will also own a private key and Certificate, which is authenticated by the CA services before access is granted.
- Surescripts CA System Administrator for registration authority duties: Requires Physical Access and is identified and authenticated by the System Access Control in place on the Surescripts CA.
- Surescripts CA Security Administrator for registration authority duties: Requires Physical Access and is identified and authenticated by the System Access Control in place on the Surescripts CA.
- Surescripts CA Operator for registration authority duties: Requires Physical Access and is identified and authenticated by the System Access Control in place on an Administrative workstation. They will also own a private key and Certificate, which is authenticated by the Surescripts CA before access is granted.
- Surescripts CA Vetter for registration authority duties: Identified and authenticated by the System Access Control in place on a predetermined and authorized workstation. They will also own a private key and Certificate, which is authenticated by the Surescripts CA services before access is granted.
- Surescripts CA Firewall Administrator: Identified and authenticated by the System Access Control in place on a predetermined and authorized workstation.
- Surescripts CA Network Administrator: Requires Physical Access and will be known to Trusted CA Roles who grant them access.
- Data Center Staff: Identified by Data Center Policy and authenticated by electronic badge access to the data center.

## 5.2.4 SEPARATION OF ROLES

Due to the multiple individuals required for tasks, a single individual may be assigned multiple roles unless stated otherwise here.

A Surescripts CA Vetter does not act as a CA System Administrator.

A Surescripts CA System Administrator or a Surescripts CA System Administrator for registration authority duties may be the same individual, but does not act in any of the following roles:

- Surescripts CA Security Administrator
- Surescripts CA Operator
- Surescripts CA Security Administrator for registration authority duties
- Surescripts CA Operator for registration authority duties
- Surescripts CA Vetter for registration authority duties
- Surescripts CA Auditor for registration authority duties

The Surescripts CA Manager will not act in any other Trusted Role for the Surescripts CA. They may act in any of the following:

- Any HSM Key Holder role
- Surescripts CA Environment Gatekeeper

The following roles will have no other roles within the Surescripts CA:

- Surescripts CA Firewall Administrator
- Surescripts CA Network Administrator
- Data Center Staff.

## 5.3 PERSONNEL CONTROLS

### 5.3.1 BACKGROUND, QUALIFICATIONS, EXPERIENCE, AND SECURITY CLEARANCE REQUIREMENTS

All persons filling trusted roles are selected on the basis of loyalty, trustworthiness, and integrity, and must be U.S. citizens.

Qualifications: Surescripts CA personnel are familiar with PKI concepts and standards, and security best practices.

Experience: Surescripts CA personnel are experienced with system and applications administration, cryptographic systems management, and security policies and procedures.

Clearance: Surescripts CA personnel are cleared for each role they act in by the Surescripts CA Manager, according to standards approved by the Surescripts Security Operations CCB.

### **5.3.2 BACKGROUND CHECK PROCEDURES**

CA personnel shall, at a minimum, pass a background investigation covering the following areas:

- Employment;
- Education;
- Place of residence;
- Law Enforcement; and
- References.

The period of investigation must cover at least the last five years for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree shall be verified.

### **5.3.3 TRAINING REQUIREMENTS**

All Surescripts CA personnel are required to complete all Surescripts employee training required of trusted employees, as well as training on this Surescripts CA CPS. All personnel operating in Surescripts CA specific roles are also required to be trained, according to their roles, in related Certificate Policies, the Surescripts CA applications, the Surescripts CA HSM, and related operating procedures. Retraining Frequency and Requirements

Individuals responsible for Trusted Roles are aware of changes in CA operation. If Surescripts operations change, Surescripts will provide a training (awareness) plan, and the execution of such plan is documented. Documentation is maintained identifying all personnel who received training and the level of training completed.

### **5.3.4 JOB ROTATION FREQUENCY AND SEQUENCE**

No stipulation.

### **5.3.5 SANCTIONS FOR UNAUTHORIZED ACTIONS**

The SRC takes appropriate administrative and disciplinary actions against personnel who violate this CPS. Sanctions for unauthorized actions on, or affecting, the Surescripts CA may range from reprimand and corrective re-training to termination and possible criminal prosecution

### 5.3.6 INDEPENDENT CONTRACTOR REQUIREMENTS

Independent contractors will be subject to same qualification, clearance, experience and training requirements as employees.

### 5.3.7 DOCUMENTATION SUPPLIED TO PERSONNEL

Surescripts CA personnel are supplied with copies (physical or electronic) of the Surescripts CA CPS and access to Surescripts CA system, application, and operations documentation, as well as standard documentation provided to Surescripts personnel.

## 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

Each audit record includes 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 information collected is listed in the table below. All security auditing capabilities of the Issuing CA operating system and CA applications required by this CPS are enabled. As a result, most of the events identified in the table are automatically recorded. Where events cannot be automatically recorded, the Surescripts CA implements manual procedures.

**Table 4. PKI Auditable Events**

Auditable Event	
<b>SECURITY AUDIT</b>	<ul style="list-style-type: none"> <li>• Any changes to the audit parameters, e.g., audit frequency, type of event audited</li> <li>• Any attempt to delete or modify the audit logs</li> </ul>



<b>Auditable Event</b>	
<b>AUTHENTICATION TO SYSTEMS</b>	<ul style="list-style-type: none"> <li>• Successful and unsuccessful attempts to assume a role</li> <li>• The value of maximum number of authentication attempts is changed</li> <li>• Maximum number of unsuccessful authentication attempts reached during user login</li> <li>• An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts</li> <li>• An administrator changes the type of authenticator, e.g., from a password to a biometric</li> </ul>
<b>LOCAL DATA ENTRY</b>	<ul style="list-style-type: none"> <li>• All security-relevant data that is entered in the system</li> </ul>
<b>REMOTE DATA ENTRY</b>	<ul style="list-style-type: none"> <li>• All security-relevant messages that are received by the system</li> </ul>
<b>DATA EXPORT AND OUTPUT</b>	<ul style="list-style-type: none"> <li>• All successful and unsuccessful requests for confidential and security-relevant information</li> </ul>
<b>KEY GENERATION</b>	<ul style="list-style-type: none"> <li>• Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys)</li> </ul>
<b>PRIVATE KEY LOAD AND STORAGE</b>	<ul style="list-style-type: none"> <li>• The loading of Component Private Keys</li> <li>• All access to certificate subject Private Keys retained within the CA for key recovery purposes</li> </ul>
<b>TRUSTED PUBLIC KEY ENTRY, DELETION AND STORAGE</b>	<ul style="list-style-type: none"> <li>• Any change to the trusted public keys, including additions and deletions</li> </ul>
<b>SECRET KEY STORAGE</b>	<ul style="list-style-type: none"> <li>• The manual entry of secret keys used for authentication</li> </ul>
<b>PRIVATE AND SECRET KEY EXPORT</b>	<ul style="list-style-type: none"> <li>• The export of private and secret keys (keys used for a single session or message are excluded)</li> </ul>
<b>CERTIFICATE REGISTRATION</b>	<ul style="list-style-type: none"> <li>• All certificate requests, including issuance, re-key, and renewal</li> <li>• Certificate issuance</li> </ul>
<b>CERTIFICATE REVOCATION</b>	<ul style="list-style-type: none"> <li>• All certificate revocation requests</li> </ul>
<b>CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION</b>	<ul style="list-style-type: none"> <li>• Certificate status change approval or rejection</li> </ul>
<b>CA CONFIGURATION</b>	<ul style="list-style-type: none"> <li>• Any security-relevant changes to the configuration of a CA system component</li> </ul>

<b>Auditable Event</b>	
<b>ACCOUNT ADMINISTRATION</b>	<ul style="list-style-type: none"> <li>• Roles and users are added or deleted</li> <li>• The access control privileges of a user account or a role are modified</li> </ul>
<b>CERTIFICATE PROFILE MANAGEMENT</b>	<ul style="list-style-type: none"> <li>• All changes to the certificate profile</li> </ul>
<b>REVOCAION PROFILE MANAGEMENT</b>	<ul style="list-style-type: none"> <li>• All changes to the revocation profile</li> </ul>
<b>CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT</b>	<ul style="list-style-type: none"> <li>• All changes to the certificate revocation list profile</li> </ul>
<b>TIME STAMPING</b>	<ul style="list-style-type: none"> <li>• A third party time stamp is obtained</li> </ul>
<b>MISCELLANEOUS</b>	<ul style="list-style-type: none"> <li>• Appointment of an individual to a Trusted Roleel for multiparty control</li> <li>• Designation of person</li> <li>• Installation of an Operating System</li> <li>• Installation of a PKI Application</li> <li>• Installation of a Hardware Security Module</li> <li>• Removal of a Hardware Security Module</li> <li>• Destruction of a Hardware Security Module</li> <li>• System Startup</li> <li>• Logon attempts to PKI Application</li> <li>• Receipt of hardware / software</li> <li>• Attempts to set passwords</li> <li>• Attempts to modify passwords</li> <li>• Backup of the internal CA database</li> <li>• Restoration from backup of the internal CA database</li> <li>• Posting of any material to a repository</li> <li>• Access to CA internal database</li> <li>• All certificate compromise notification requests</li> <li>• Loading tokens with certificates</li> <li>• Shipment of tokens</li> <li>• Zeroizing HSMs</li> <li>• Re-key of the Component</li> </ul>

<b>Auditable Event</b>	
<b>CONFIGURATION CHANGES</b>	<ul style="list-style-type: none"> <li>• Hardware</li> <li>• Software</li> <li>• Operating System</li> <li>• Patches</li> <li>• Security profiles</li> </ul>
<b>PHYSICAL ACCESS / SITE SECURITY</b>	<ul style="list-style-type: none"> <li>• Personnel access to room housing CA</li> <li>• Access to the CA server</li> <li>• Known or suspected violations of physical security</li> </ul>
<b>ANOMALIES</b>	<ul style="list-style-type: none"> <li>• System crashes and hardware failures</li> <li>• Software error conditions</li> <li>• Software check integrity failures</li> <li>• Receipt of improper messages</li> <li>• Misrouted messages</li> <li>• Network attacks (suspected or confirmed)</li> <li>• Equipment failure</li> <li>• Electrical power outages</li> <li>• Uninterruptible power supply (UPS) failure</li> <li>• Obvious and reported network service or access failures</li> <li>• Violations of a CP or CPS</li> <li>• Resetting Operating System clock</li> </ul>

#### **5.4.2 FREQUENCY OF PROCESSING LOG**

The Surescripts CA logs are rolled daily (the previous day's logs are archived and a new log is begun). Auto-vetting log files are rolled when they reach or exceed a preset size, for example, one megabyte. System log roll-over is controlled by configuration settings managed by the system administrators. Archived log files are processed monthly.

#### **5.4.3 RETENTION PERIOD FOR AUDIT LOGS**

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

#### **5.4.4 PROTECTION OF AUDIT LOGS**

Only authorized personnel (CA administrators and auditors) have access to the logs, and only authorized personnel archives the logs. CA configuration and access control processes enforce these requirements.

#### **5.4.5 AUDIT LOG BACKUP PROCEDURES**

Security audit data are backed up at least monthly and stored off-site in a redundant CA repository maintained in a data center grade environment.

#### **5.4.6 AUDIT COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)**

All security audit processes are invoked at CA startup and cease only at shutdown. Should it become apparent that an automated security audit system has failed; the CA ceases 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 CPS.

#### **5.4.8 VULNERABILITY ASSESSMENTS**

A formal vulnerability assessment was used to guide the design of the Surescripts CA systems and their security controls and safeguards.

Periodic vulnerability assessments are conducted at least annually.

### **5.5 RECORDS ARCHIVAL**

#### **5.5.1 TYPES OF EVENTS ARCHIVED**

CA archive records are sufficiently detailed as to verify that the CA was properly operated as well as to verify the validity of any certificate throughout its validity period. At a minimum, the following data is 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 are kept for a minimum of ten years & 6 months.

### **5.5.3 PROTECTION OF ARCHIVE**

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

### **5.5.4 ARCHIVE BACKUP PROCEDURES**

CA/RA servers are subject to a common server backup procedure using CommVault data protection software and used for all server assets within the enterprise. This includes a weekly FULL backup that is retained for 30 days.

This is same backup procedure for any of the items mentioned in 5.5.1 as are archived to file server shares.

### **5.5.5 REQUIREMENTS FOR TIME-STAMPING OF RECORDS**

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

### **5.5.6 ARCHIVE COLLECTION SYSTEM (INTERNAL VS. EXTERNAL)**

No stipulation.

### **5.5.7 PROCEDURES TO OBTAIN & VERIFY ARCHIVE INFORMATION**

All CA/RA data archived can be browsed for validation|restore using the CommVault browse|recovery tool as administered by the Surescripts Sytems Engineering team. Details on this are found in the CommVault administration procedures located within the Surescripts Information Security Policy and Procedures Library.

## **5.6 KEY CHANGEOVER**

The CA does not issue Subscriber certificates that extend beyond the expiration date of its own CA certificates and public keys, and the CA certificate validity period extends 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 is changed more frequently, and only the new key is used for certificate signing purposes from that time. The older, but still valid, certificate is 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 is retained and protected.

The CA self-signed root certificate is valid for 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 is 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 are followed. Otherwise the scope of potential damage is assessed in order to determine if the CA needs to be rebuilt, only some certificates need to be revoked, and/or the CA key needs to be declared compromised.

The Federal PKI Policy Authority shall be notified if any CAs operating under this policy experience the following:

- suspected or detected compromise of the CA systems;
- suspected or detected compromise of a certificate status server (CSS) if (1) the CSS certificate has a lifetime of more than 72 hours and (2) the CSS certificate cannot be revoked (e.g., an OCSP responder certificate with the id-pkix-ocsp-nocheck extension);
- physical or electronic penetration of CA systems;
- successful denial of service attacks on CA components; or
- any incident preventing the CA from issuing a CRL within 48 hours of the issuance of the previous CRL.

The CA's Operational Authority shall reestablish operational capabilities as quickly as possible in accordance with procedures set forth in the CA's CPS.

### **5.7.2 COMPUTING RESOURCES, SOFTWARE, AND/OR DATA ARE CORRUPTED**

The CA maintains 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 is 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 shall have recovery procedures in place to reconstitute the CA within 72 hours of failure.

If the CA cannot reestablish revocation capabilities prior to the next update field in the latest CRL issued by the CA, then the SRC decides 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 is completely rebuilt by reestablishing the CA equipment and generating new private and public keys. Finally, all Subscriber certificates are 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

For Surescripts Certificates:

In the event of CA termination, certificates signed by the CA are revoked.

For Surescripts TLS Certificates:

The CA shall provide archived data to an archive facility.

When the CA operating under this policy terminates operations before all certificates have expired, the CA signing keys shall be surrendered to the Federal PKI Policy Authority. Prior to CA termination, the CA shall provide archived data to an archive facility as specified in the CPS. As soon as possible, the CA will advise all other organizations to which it has issued certificates of its termination, using an agreed-upon method of communication specified in the CPS.



---

## SECTION 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 are generated on a tamper-proof hardware secure module (HSM)

##### 6.1.1.2 SUBSCRIBER KEY PAIR GENERATION

The CA cryptographic keying material generated for Subscriber certificates is created on physical hardware that is rated at a FIPS 140-2 level 2.

#### 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

The CA root public key is delivered within a self-signed certificate using a commercially reasonable out-of-band medium trusted by the relying party (email).

#### 6.1.5 KEY SIZES

The Surescripts CA generates and use the following keys, signature algorithms, and hash algorithms for signing certificates, CRLs, and certificate status server responses:

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

All but the first-listed above is utilized for Subscriber keys.

The Surescripts CA issues end-entity certificates that contain at least 2048-bit public keys for RSA, DSA, or Diffie-Hellman, or at least 224 bits for elliptic curve

algorithms, except for certificates issued to smart cards or other hardware devices that are incapable of accepting 2048-bit RSA certificates.

### 6.1.6 PUBLIC KEY PARAMETERS GENERATION AND QUALITY CHECKING

The Surescripts CA generates 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)

<b>Surescripts CA</b>	
Subscriber Certificates	Surescripts CA public keys that are bound into certificates are certified for use in signing and encryption of S/MIME packages. Specifically, Subscriber certificates assert the following key usage bits:
	<ul style="list-style-type: none"> <li>digitalSignature</li> </ul>
	<ul style="list-style-type: none"> <li>KeyEncipherment: Subscriber certificates that are dual-use certificates do not assert the non-repudiation bit.</li> </ul>
	Subscriber certificates also assert an extended key usage bit of <i>emailProtection</i> and a BasicConstraint of <i>CA:FALSE</i> .
Root Certificate	The Surescripts CA root certificate asserts the following key usage bits:
	<ul style="list-style-type: none"> <li>cRLSign</li> </ul>
	<ul style="list-style-type: none"> <li>keyCertSign</li> </ul>
	The Surescripts CA root certificate also asserts a Basic Constraint of <i>CA:TRUE</i> .
<b>Surescripts Issuing CA</b>	
Subscriber Certificates	Surescripts Issuing CA public keys that are bound into certificates are certified for use in client

	authentication and server authentication. Subscriber certificates assert the following key usage bits:
	<ul style="list-style-type: none"> <li>• digitalSignature</li> </ul>
	<ul style="list-style-type: none"> <li>• KeyEncipherment: Subscriber certificates that are dual-use certificates do not assert the non-repudiation bit.</li> </ul>
	<ul style="list-style-type: none"> <li>• TLS Web Server Authentication</li> </ul>
	<ul style="list-style-type: none"> <li>• TLS Web Client</li> </ul>
	Subscriber certificates also assert a BasicConstraint of <i>CA:FALSE</i> .
Root Certificate	The Surescripts Issuing CA root certificate asserts the following key usage bits:
	<ul style="list-style-type: none"> <li>• cRLSign</li> </ul>
	<ul style="list-style-type: none"> <li>• keyCertSign</li> </ul>
	<ul style="list-style-type: none"> <li>• Off-line CRL Signing</li> </ul>
	The Surescripts Issuing CA root certificate also asserts a Basic Constraint of <i>CA:TRUE</i> .

## 6.2 PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

### 6.2.1 CRYPTOGRAPHIC MODULE STANDARDS AND CONTROLS

All HSMs are validated to the 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 (CA or Subscriber) are not escrowed.

## **6.2.4 PRIVATE KEY BACKUP**

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

Subscriber private keys are backed up to a redundant 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**

Once the HSM has been turned on, the private key may be used by the application. The private key is available for use until the application is stopped or other interruption of service occurs (e.g. shutdown).

The Surescripts HSM Operator key Holders can activate the private keys.

## **6.2.9 METHODS OF DEACTIVATING PRIVATE KEYS**

The Surescripts CA deactivates its Private Keys and stores its off-line HSMs in secure containers when not in use. The Surescripts CA prevents unauthorized access to any activated cryptographic modules.

## **6.2.10 METHOD OF DESTROYING PRIVATE KEYS**

CA Administrators destroy private signature keys when they are no longer needed.

Subscriber private signature keys are 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

The Surescripts CA root private key is used for a maximum of 20 years. It expires after a maximum of 10 years.

Surescripts Direct Certificates	Private keys	Subscriber private keys are used for a maximum of 4 years.
	Subscriber	Subscriber public certificates expire after two years.
Surescripts TLS Certificates	Root	Root certificates expire after 20 years.
	Subscriber	Subscriber certificates expire after two years.

For OCSP responders operating under this policy and all other subscriber public keys, the maximum usage period is three years.

## **6.4 ACTIVATION DATA**

### **6.4.1 ACTIVATION DATA GENERATION AND INSTALLATION**

The Surescripts CA or Subscriber generates activation data that has 13 randomly generated characters to protect its respective Private Keys.

If the activation data must be transmitted, it shall be via an appropriately protected channel, and distinct in time and place from the associated cryptographic module.

### **6.4.2 ACTIVATION DATA PROTECTION**

The Surescripts CA protects data used to unlock private keys from disclosure using a tamper-proof HSMs and physical access control mechanisms. Activation data is recorded and secured at the level of assurance associated with the activation of the cryptographic module, and is not stored with the cryptographic module.

The Surescripts CA requires personnel to memorize and not write down their password. The Company protects all shared secrets and has implemented 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 Surescripts CA configures its CA systems, including any remote workstations, to:

- authenticate the identity of users 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 for all transactions,
- enforce domain integrity boundaries for security critical processes, and
- Support recovery from key or system failure.

The Surescripts CA authenticates and protects 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**

All CA software was purchased from recognized software and hardware manufacturers. These applications are dedicated to performing CA functions. The protection of CA hardware and software containing private keys is part of the terms for Subscriber and Trusted Role Agreement Forms.

Hardware and software procured to operate the CA shall be purchased in a fashion to reduce the likelihood that any particular component was tampered with (*e.g., by ensuring the vendor cannot identify the PKI component that will be installed on a particular device*).

### **6.6.2 SECURITY MANAGEMENT CONTROLS**

The configuration of a CA system as well as any modifications and upgrades are documented and controlled through Change Control Practices. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system.

The firewall protecting the Surescripts CA system from external networks is managed by a Surescripts Operations firewall expert, under the supervision of the Surescripts CA Manager. Firewall logs are collected and analyzed periodically. KMS-0706, Firewall Rule Set, defines the firewall configuration and management.

A centralized security management tool (procured from Symantec) is run on the computers of the Surescripts CA system to enforce access policies, manage user accounts, and log significant events. A set of Information technology (IT) procedures, approved by Security Operations CCB, govern operations of the Surescripts CA system computers.

### **6.6.3 LIFE CYCLE SECURITY RATINGS**

No stipulation.

## 6.7 NETWORK SECURITY CONTROLS

Information to be transferred from the Surescripts CA is done through dedicated removable media or secure networks. The Surescripts CA signing servers are isolated from the Surescripts business network by a dedicated firewall. Certificate requests move from the intranet to the Surescripts CA signing servers through the firewall or by manual means. Certificate requests are mediated by the Surescripts CA where they are screened for validity. The resulting Certificates are returned by the Surescripts CA to the subscriber through the Surescripts firewall or by manual means.

Any boundary control devices used to protect the network on which PKI equipment is hosted shall deny all but the necessary services to the PKI equipment.

Directories, certificate status servers, and remote workstations used to administer the CAs shall employ appropriate network security controls. Networking equipment shall turn off unused network ports and services. Any network software present shall be necessary to the functioning of the equipment.

The CA shall establish connection with a remote workstation used to administer the CA only after successful authentication of the remote workstation at a level of assurance commensurate with that of the CA.

## 6.8 STAMPING

The system clock time for the CA system is derived from a trusted time service. This CA is implemented as a Microsoft Active Directory Certification Services CA, where all member servers and domain controllers sync to a domain controller holding Primary Domain Controller (PDC) Emulator role. The PDC Emulator role syncs to an external source 'stime.windows.com' every 10 minutes.

Asserted times shall be accurate to within three minutes.



---

## SECTION 7 CERTIFICATE, CRL, AND OCSP PROFILE FORMATS

---

### 7.1 CERTIFICATE PROFILE

#### 7.1.1 VERSION NUMBERS

The Surescripts CA issues X.509 v3 certificates, which means the version field should contain the integer 2.

#### 7.1.2 CERTIFICATE EXTENSIONS

The Surescripts CA uses standard certificate extensions that are compliant with IETF RFC 5280.

- The Key Usage, Extended Key Usage, and Basic Constraints extensions is populated as specified in section 6.1.7 of the Surescripts CA Certificate Policy.
- The CRL Distribution Points extension may be populated with a CRL URL as specified in section 2.2.1 of the Surescripts CA Certificate Policy.
- The Authority Information Access extension may be populated with an OCSP Responder location as specified in section 2.2.1 of the Surescripts CA Certificate Policy.
- The Subject Alternative Name extension is populated as specified in section 3.1.1 of the Surescripts Certificate Policy.
- The Certificate Policies extension is populated as defined in section 7.1.6 of the Surescripts Certificate Policy.

#### 7.1.3 ALGORITHM OBJECT IDENTIFIERS

End Entity Certificates signed by the Surescripts CA uses 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 the Surescripts 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 Surescripts CA CPS.

#### **7.1.5 NAME CONSTRAINTS**

No stipulation.

#### **7.1.6 CERTIFICATE POLICY OBJECT IDENTIFIER**

Certificates assert at least one of the policy OIDs (or a policy OID of a superior CP that has been successfully mapped to the DirectTrustCP) defined in section 1.2 of the Certificate Policy.

#### **7.1.7 USAGE OF POLICY CONSTRAINTS EXTENSION**

No stipulation.

#### **7.1.8 POLICY QUALIFIERS SYNTAX AND SEMANTICS**

No stipulation.

#### **7.1.9 PROCESSING SEMANTICS FOR THE CRITICAL CERTIFICATE POLICY EXTENSION**

The Surescripts CA Certificate 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**

The Surescripts CA issues X.509 version 2 CRLs, which means the version field should contain the integer 1.

#### **7.2.2 CRL AND CRL ENTRY EXTENSIONS**

The Surescripts CA conforms to the CRL and CRL Extensions profile defined in IETF RFC 5280.

The Surescripts CA signs the CRL using the SHA-256 signature algorithm and identify it using the following OID:

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

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

## 7.3 OCSP PROFILE

The status of public certificates is available via a CRL or OCSP responder. These services are included in an high availability (HA) cluster where responders are available concurrently in multiple data center locations.

---

## SECTION 8 **COMPLIANCE AUDITS AND OTHER ASSESSMENTS**

---

The Surescripts CA has a compliance audit mechanism in place to ensure that the requirements of their CP/CPS are being implemented and enforced. Surescripts uses a compliance auditor that is independent from the CA.

Surescripts provides a DirectTrust/EHNAC supplied assertion package to make a self-attested, legally binding Declaration of Conformance to this CPS.

The practices in this CPS are designed to meet or exceed the requirements of the latest version of the CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

### **8.1 INDEPENDENT AUDIT FOR PKI OPERATION**

Annually, Surescripts PKI practices and infrastructure will undergo a Webtrust Audit. The audit occurs at least once per year.

### **8.2 IDENTITY/QUALIFICATIONS OF ASSESSOR**

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA's CPS and CP. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

The CA Declaration of Conformance describes the compliance assessor's relationship to the CA, indicating that the assessor is an independent compliance auditor

### **8.3 ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY**

The CA Declaration of Conformance describes the compliance assessor is an independent compliance auditor. If DirectTrust provides an accreditation program to certify the compliance of CAs, RAs, and HISPs, in which case the Surescripts CA adheres to this program.

## **8.4 TOPICS COVERED BY ASSESSMENT**

The purpose of a compliance audit shall be to verify that a CA and its recognized RAs comply with all the requirements of the current versions of the CP and the CA's CPS. All aspects of the CA/RA operation shall be subject to compliance audit inspections.

## **8.5 ACTIONS TAKEN AS A RESULT OF DEFICIENCY**

Surescripts takes all items of non-conformance seriously. For every item of non-conformance, Surescripts drafts a Mitigation Plan including level of effort and expected resolution.

The party responsible for correcting the discrepancy will propose a remedy, including expected time for completion, to the FPKIPA and appropriate Relying Parties.

The Audit Compliance Report and identification of corrective measures shall be provided to both the SRC and any third party that Surescripts is legally obligated to satisfy.

The information contained in compliance reports and restricted to the Surescripts SRC and Relying Parties on a need to know basis only.

## **8.6 COMMUNICATION OF RESULTS**

The information contained in compliance reports and restricted to the Surescripts SRC and Relying Parties on a need to know basis only.

Surescripts provides a link to a web page for the CAs to publish where its Declaration of Conformance is available.

---

## **SECTION 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**

All data and their hardware containers are considered proprietary and confidential. Handling corresponds to Surescripts policies for this classification of data. These include:

- Certificate application records.
- Transactional records (both full records and audit trail of transactions)
- Audit trail records created or retained by Surescripts or a customer
- Audit reports created by Surescripts or a Customer (to the extent such reports are maintained), or their respective auditors (whether internal or public)
- Contingency planning and disaster recovery plans
- Security measures controlling the operations of Surescripts hardware and software and the administration of Certificate services and designated enrollment services.

### **9.3.2 INFORMATION NOT WITHIN THE SCOPE OF CONFIDENTIAL INFORMATION**

The Surescripts CA treats all information in the CPS as confidential and proprietary information.

### **9.3.3 RESPONSIBILITY TO PROTECT CONFIDENTIAL INFORMATION**

The Surescripts CA contractually obligate employees, agents, and contractors to protect confidential information through its Trusted Role Agreement. Surescripts provides 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 is protected from unauthorized disclosure. The Surescripts CA creates and follows a publicly posted privacy policy at <http://surescripts.com/privacy-policy> that specifies how it 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.

#### **9.4.3 INFORMATION NOT DEEMED PRIVATE**

Information included in certificates is not deemed private.

#### **9.4.4 RESPONSIBILITY TO PROTECT PRIVATE INFORMATION**

The Surescripts CA stores private information securely.

#### **9.4.5 NOTICE AND CONSENT TO USE PRIVATE INFORMATION**

The Surescripts CA uses private information as dictated by their Clinical Interoperability Agreements with its Subscribers.

#### **9.4.6 DISCLOSURE PURSUANT TO JUDICIAL/ADMINISTRATIVE PROCESS**

The Surescripts CA does 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**

Surescripts and the Surescripts CA do not knowingly violate the intellectual property rights held by others.

### **9.6 REPRESENTATIONS AND WARRANTIES**

#### **9.6.1 CA AND RA REPRESENTATIONS AND WARRANTIES**

The Surescripts CA will use reasonable efforts to provide the services described herein in an efficient and trustworthy manner. The Surescripts CA will take reasonable precautions to protect the confidentiality of its private keys and other information used to create Certificates.



By issuing a Certificate to a Subscriber, the Surescripts CA represents to the Subscriber, and to all qualified Relying Parties who depend on the information contained in the Certificate, that during its period of validity:

- The Surescripts CA will issue and revoke Certificates in accordance with this Surescripts CA CPS and any applicable CP when required.
- There will be no material misrepresentations of fact or errors in the Certificate as a result of the Surescripts CA's failure to use reasonable care in creating the Certificate, and the Surescripts CA will take reasonable steps to confirm the accuracy of the information in the Certificate.
- The Surescripts CA will accurately transcribe information provided by the Applicant (as defined in Section 1.3.5) in the Certificate application to the Certificate.
- The Subscriber's public and private key will constitute a functional key pair.
- The Subscriber holds the private key that corresponds to the public key listed in his/her Certificate.
- The Surescripts CA has a trustworthy system to generate, issue, and publish the Certificate.
- The Surescripts CA will revoke Certificates pursuant to the terms and conditions of this Surescripts CA CPS and any applicable CP.
- The Certificates will be reasonably fit for their intended use within the PKI for the Surescripts business.
- The Surescripts CA will process Certificate applications pursuant to the Surescripts CA CPS and any other applicable documentation.
- The Surescripts RA will request Certificates be issued by the Surescripts CA for a Subscriber verified in accordance with this Surescripts CA CPS.
- The Surescripts CA will comply with this Surescripts CA CPS.
- The Surescripts CA will give a copy of this Surescripts CA CPS and a Subscriber Agreement to each Subscriber, or direct the Subscriber to where they may get their own copies of these documents.
- The Surescripts CA will process Certificate revocation requests and submit properly vetted revocation requests to the Surescripts CA in accordance with this Surescripts CA CPS

## **9.6.2 RA REPRESENTATIONS AND WARRANTIES**

See 9.6.1

### **9.6.3 SUBSCRIBER REPRESENTATIONS AND WARRANTIES**

Each Subscriber represents to the Surescripts 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.
7. Promptly notify the appropriate CA upon suspicion of loss or compromise of their private key(s). Such notification shall be made directly or indirectly through mechanisms consistent with the CA's CPS.

Wherever possible, subscriber documents must be digitally signed.

If the human sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device's private key and ensure that the device's certificate is only used for authorized purposes, the device sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation shall be documented and signed by both the device sponsor and the authorized administrator for the device. Delegation does not relieve the device sponsor of his or her accountability for these responsibilities.

### **9.6.4 RELYING PARTIES REPRESENTATIONS AND WARRANTIES**

Relying parties use a Surescripts 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**

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

## **9.9 INDEMNITIES**

No stipulation.

## **9.10 TERM AND TERMINATION**

### **9.10.1 TERM**

This CPS becomes effective when approved through the Surescripts consensus process. This CPS has no specified term.

### **9.10.2 TERMINATION**

Termination of this Certification Practice Statement may occur if approved through the Surescripts consensus process.

### **9.10.3 EFFECT OF TERMINATION AND SURVIVAL**

The requirements of this Certification Practice Statement 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 Certification Practice Statement may be amended through the Surescripts approval 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 Certification Practice Statement, a statement of guidance may be issued and published on the Surescripts website if approved through the Surescripts consensus process.

## **9.14 GOVERNING LAW**

The laws of the United States of America shall govern this Certification Practice Statement.

## **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 Certification Practice Statement is incorrect or invalid, the other sections of this Certification Practice Statement shall remain in effect until the Certification Practice Statement 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.

