HISP Practices Statement



South Carolina Health Information Exchange

Table of Contents

[1 Introduction 3](#_Toc501610340)

[1.1 Overview 3](#_Toc501610341)

[1.2 Document Name and Identification 3](#_Toc501610342)

[1.3 Definitions and Acronyms 3](#_Toc501610343)

[1.3.1 Definitions 3](#_Toc501610344)

[1.3.2 Acronyms 4](#_Toc501610345)

[1.3.3 References 4](#_Toc501610346)

[2 Implementation Standards 4](#_Toc501610347)

[3 Certificate and Key Management 4](#_Toc501610348)

[3.1 Information Systems Security Officer 4](#_Toc501610349)

[3.2 Appropriate Certificate Uses 4](#_Toc501610350)

[3.3 Certificate Authority and Registration Authority Services 5](#_Toc501610351)

[3.4 Certificate Life-Cycle Operational Requirements 5](#_Toc501610352)

[3.5 Public Key Accessibility 5](#_Toc501610353)

[3.6 Private Key Security 5](#_Toc501610354)

[4 Trust Management 5](#_Toc501610355)

[4.1 HISP Administrator 5](#_Toc501610356)

[4.2 Trust Establishment 5](#_Toc501610357)

[5 Facility, Management, and Operational Controls 6](#_Toc501610358)

[5.1 Physical Controls 6](#_Toc501610359)

[5.1.1 Physical Security 6](#_Toc501610360)

[5.1.2 Power and Air Conditioning 6](#_Toc501610361)

[5.1.3 Water Exposure 7](#_Toc501610362)

[5.1.4 Fire Detection & Prevention 7](#_Toc501610363)

[5.1.5 Off-site Backup 7](#_Toc501610364)

[5.2 Procedural Controls 7](#_Toc501610365)

[5.3 Personnel Controls 7](#_Toc501610366)

[5.4 Audit Logging 7](#_Toc501610367)

[6 Technical Security Controls 8](#_Toc501610368)

# Introduction

## Overview

Direct Messaging is a method for secure transmission of protected health information (PHI) over the internet. This document outlines the general policy guidelines the SCHIEx Health Information Service Provider (HISP) follows in operating Direct Messaging services for its end users. This document is not intended to replace or alter any existing policies and practices that SCHIEx has in place, but rather speaks to the specifics relating to its’ Direct Messaging services.

## Document Name and Identification

This document is the SCHIEx HISP Practices Statement and was first approved for publication in November 2017 by the SCHIP CEO. The following revisions have been made to the original document:

|  |  |  |
| --- | --- | --- |
| **Date** | **Changes** | **Version** |
| 6/6/2018 | Updated links to Digicert’s policies | 1.1 |
| 7/10/2019 | Reviewed, no changes made | 1.1 |
| 10/5/2021 | Reviewed, no change made | 1.1 |

## Definitions and Acronyms

### Definitions

“**Certificate**” is an electronic document that uses a digital signature to bind a Public Key and an identity.

“**Cloning Domain**” is a group of Hardware Security Modules

“**Direct Address**” is an email address conforming to the Applicability Statement for Secure Health

Transport.

“**Direct Address Certificate**” is a Certificate containing an entire Direct Address.

“**Hardware Security Module**” is a physical computing device that safeguards, manages digital keys for strong authentication, and provides crypto processing.

“**Key Pair**” is a Private Key and associated Public Key.

“**Partition**” is an encrypted storage area within the HSM where objects such as keys are stored.

“**Private Key**” is the key of a Key Pair that is kept secret by the holder of the Key Pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

“**Public Key**” is the key of a Key Pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

**“Relying Party”** is the entity that acts in reliance on a Certificate and/or digital signature issued by

the Issuer CA. Relying parties must check the appropriate CRL or OCSP response prior to relying on

information featured in a Certificate.

### Acronyms

CA Certificate Authority

CRL Certificate Revocation List

CSR Certificate Signing Request

FIPS (US Government) Federal Information Processing Standard

FQDN Fully Qualified Domain Name

HCO Healthcare Organization

HSM Hardware Security Module

ISSO Information System Security Officer

OCSP Online Certificate Status Protocol

SFTP Secure File Transfer Protocol

SHA Secure Hashing Algorithm

SO Security Officer

SSL Secure Socket Layer

TLS Transport Layer Security

### References

[DigiCert Certificate Policy Version 4.14](https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CP_v414.pdf)

SCHIEx Policies and Procedures – March 16, 2017 Revision

# Implementation Standards

The SCHIEx HISP implements the standards outlined in the following specifications for DIRECT Messaging:

* [Applicability Statement for Secure Health Transport v1.2](http://wiki.directproject.org/file/view/Applicability+Statement+for+Secure+Health+Transport+v1.2.pdf)
* [XDR and XDM for Direct Messaging v1.0](http://wiki.directproject.org/file/view/2011-03-09%20PDF%20-%20XDR%20and%20XDM%20for%20Direct%20Messaging%20Specification_FINAL.pdf)
* [Implementation Guide for Delivery Notification in Direct v1.0](http://wiki.directproject.org/file/view/Implementation+Guide+for+Delivery+Notification+in+Direct+v1.0.pdf)

# Certificate and Key Management

## Information Systems Security Officer

The SCHIEx Information Systems Security Officer is responsible for ensuring adequate protection of and managing access to the cryptographic keys used by the DIRECT Messaging services. As of November 2017, the SCHIEx ISSO is Elizabeth Hall.

## Appropriate Certificate Uses

Certificates may be used for encryption, access control, and digital signature purposes for SCHIEx DIRECT secure messaging.

The SCHIEx HISP strictly adheres to the key usage field on Direct certificates when marked critical.

The SCHIEx HISP supports both single and dual-use certificates for the purpose of signing outbound messages and decrypting inbound messages.

## Certificate Authority and Registration Authority Services

SCHIEx has partnered with DigiCert for Certificate Authority (CA) and Registration Authority (RA) services. Please refer to Sections 3 and 4 of the [DigiCert Certification Practices Statement](https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CPS_v414.pdf) for more information.

## Certificate Life-Cycle Operational Requirements

As the SCHIEx CA for Direct messaging, DigiCert handles certificate application processing, issuance, renewal, re-keying, modification, revocation and suspension. Please refer to Section 4 of the [DigiCert Certification Practices Statement](https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CPS_v414.pdf) for more information.

SCHIEx is contractually obligated to protect its Private Keys from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated Certificate, and use Certificates in accordance with their intended purpose.

A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate.

## Public Key Accessibility

The SCHIEx HISP strictly adheres to the [Applicability Statement for Secure Health Transport v1.2](http://wiki.directproject.org/file/view/Applicability+Statement+for+Secure+Health+Transport+v1.2.pdf) and all public keys used by the SCHIEx HISP for encrypting DIRECT Messages are made available over DNS.

The SCHIEx HISP strictly adheres to the key usage field on Direct certificates when marked critical.

## Private Key Security

Private keys used by the SCHIEx HISP for signing and decrypting DIRECT Messages are generated and stored in hardware security modules that are certified to Federal Information Processing Standard (FIPS) 140-2 Level 2.

All keys must be generated by and in a cryptographic HSM. The private keys never leave the HSM. A remote backup HSM is connected to the production HSM. The keys are generated on the remote cryptographic HSM and then securely backed up and restored to the production cryptographic HSM.

# Trust Management

## HISP Administrator

SCHIEx has individuals responsible for administrating the DIRECT Messaging services. These individuals are responsible for enabling and disabling trust by means of whitelisting trust anchors and trust bundles that the HISP can communicate with. Additionally, the HISP Administrator is responsible for granting end-user access and mailbox creation.

## Trust Establishment

SCHIEx HISP manages trust anchors and trust bundles for its DIRECT participants to facilitate end user exchange of DIRECT messages among SCHIEx member participants and with external counterparties. The SCHIEx organizations as members of its trust network chain to the SCHIEx intermediate certificate and trust one another. SCHIP has established a policy to enable trust with DIRECT service providers who are either 1) part of the DirectTrust Accredited Trust Bundle; 2) have been otherwise approved by SCHIP; or 3) who have been approved by a member participant who has an exclusive trust relationship with the entity and trust may be established between these parties if approved by SCHIP.

As a relying party, and using SCHIP’s fully executed agreement with DigiCert, prior to relying on the information listed in a Certificate, SCHIEx confirms the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer‐to‐subject name chaining, policy and key use constraints, and revocation status through CRLs or OCSP responders identified in each Certificate in the chain. HISP-to-HISP Agreements are maintained for established trusts.

# Facility, Management, and Operational Controls

SCHIP contracts with the SC Revenue & Fiscal Affairs Office (RFA) to provide hosting, architectural, and administrative support to the SCHIEx platform. RFA utilizes an external data center to host the SCHIEx infrastructure. The datacenter adheres to RFA’s physical security and access control policies.

RFA has a full Information Technology team, covering the architectural and administrative support of SCHIEx, as well as, security and the ISSO role for DIRECT messaging. RFA also assists SCHIP with managing web portal access and reporting. SCHIP also contracts with CareEvolution for development and support of the SCHIEx software. CareEvolution has a team of developers that specialize in the different components of the SCHIEx platform. SCHIP has staff that serves as the primary liaison between SCHIEx participants and vendors, as well as other partners.

## Physical Controls

### Physical Security

The datacenter is equipped with physical controls that make SCHIEx operations inaccessible to non-trusted personnel. SCHIP and RFA operate under security policies designed to detect, deter, and prevent unauthorized access to SCHIEx operations.

RFA protects the SCHIEx equipment from unauthorized access and implements physical controls to reduce risk of equipment tampering. The secure parts of the data center are protected using physical access controls making them accessible only to appropriately authorized individuals.

Physical security is provided to the facility 24x7x365. Visitor sign in sheets and ID checks are maintained at the security desk. A card reader system restricts movement of personnel to various areas of the building. Keys and combinations will be given only to those individuals, preferably supervisors, who have a frequent need to access the area after duty hours. Hours for access of approved personnel shall be 24x7x365.

The data center has no exterior windows.

### Power and Air Conditioning

The datacenter building is fed from a single service provided by a utility company. A diesel generator is provided for the entire data center load. This generator will provide all power for the computer loads, lighting loads, and HVAC loads. Automatic transfer switches will switch to generator power upon loss of normal power from the facility. Uninterrupted power supplies (UPS) provide redundant backup power. All computer room power is designed to provide a continuous source of electricity should power be interrupted at any transmission point with the room.

The data center uses a dedicated redundant HVAC system.

### Water Exposure

The data center is located above street level so the risk of flooding is very low.

### Fire Detection & Prevention

The data center is equipped with fire detection mechanisms. Manual fire suppressants are properly placed and fully charged.

### Off-site Backup

RFA maintains makes regular backup copies of any information necessary to recover from a system failure. Encrypted backup copies of systems, data, and private keys are stored for disaster recovery purposes off-site and are accessible only by trusted personnel.

## Procedural Controls

RFA maintains an access control procedure for SCHIEx with supplemental separation of duties matrix and list of personnel that are authorized to access the SCHIEx system.

## Personnel Controls

RFA performs background checks on all personnel during the hiring process. All personnel are required to complete annual HIPAA privacy training and security awareness training.

All SCHIEx contractors shall use its best efforts to avoid viewing or accessing protected health information, including individually identifiable information.  However, in the event that Contractor is required to view or access such information to facilitate participant connections, Contractor shall comply with all applicable federal and state laws and regulations regarding the confidential and secure treatment of protected health information, including but not limited to the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), in particular the Standards for Privacy of Individually Identifiable Health Information (45 C.F.R. Parts 160 and 164, as amended), the Standards for Electronic Transactions (45 C.F.R. Parts 160 and 162), and the Security Standards (45 C.F.R. Parts 160, 162 and 164).

## Audit Logging

The SCHIEx platform audits the following events:

|  |
| --- |
| **Domain:** |
| Logon Events |
| Account Management Events |
| Object Access |
| Policy Change |
| Privilege Functions |
| System Events |
| **Application:** |
| All Activity |
| Logon Events |
| Data Access |
| Permission Changes |

The SCHIEx infrastructure utilizes the NIST time service to ensure accuracy and precision of timestamps in the audit records.

RFA retains audit logs for any activity that is subject to HIPAA for 6 years.

# Technical Security Controls

SCHIP works with each HCO to create an account for them in the DigiCert web portal. Each HCO must have a designated representative that will be subject to identity verification by DigiCert, as outlined in section 3.2 of the [DigiCert Certification Practices Statement](https://www.digicert.com/wp-content/uploads/2018/01/DigiCert_CPS_v414.pdf). Requests for organizational certificates will not be approved by DigiCert until the identity verification is complete.

SCHIEx uses for secure DIRECT messaging the domain: direct.schiex.state.sc.us

All HCOs will be assigned a subdomain to direct.schiex.state.sc.us. The subdomain will be named to reflect the name of the HCO. DigiCert must approve all subdomains.

RFA submits to DigiCert the CSR that has been generated on the cryptographic HSM for both the encryption and signing certificate. The SCHIEx ISSO approves the request for the DigiCert organizational certificate.

Once DigiCert issues the certificates, RFA downloads them and places them back onto the cryptographic HSM via SFTP. The DigiCert certificates are then placed back with the private keys on the cryptographic HSM for use by the SCHIEx application.

The SCHIEx infrastructure utilizes the NIST time service to ensure accuracy and precision in the HISP environment.

The SCHIEx web portal requires all end users to authenticate in a secure manner before performing any actions, such as accessing their direct secure messaging mailbox.  All intermediate systems communicate exclusively over secure channels.  Any and all actions (including users authentication) are audit logged. Please refer to SCHIEx Policies and Procedures, Section 12 for more detail on access to SCHIEx.