HSPD-12 Shared Component Infrastructure Trust Model

Version 1.0.1
December 14, 2006

FINAL

Document History

Status	Release	Date	Comment	Audience
Initial	0.0.1	05/18/06	Internal Review	Enspier
Strawman	0.0.2	05/18/06	Internal Review	Enspier
Strawman	0.0.3	05/23/06	AWG initial release for comments	AWG
Draft	0.0.4	05/30/06	Revised per AWG comments	Enspier
Draft	0.0.5	05/31/06	Revised per AWG comments	AWG
Draft	0.0.6	08/21/06	Revised per AWG comments	AWG
Draft	0.1.0	08/31/06	Released for public review.	Public
Draft	0.1.1	10/20/06	Updated per public comments, AWG guidance, and further internal review	AWG
Draft	0.1.2	10/31/06	Enhanced Section 2.5, Security Principles, to address NIST SP 800-95.	AWG
Final	1.0.0	11/16/06	Final Version	Public
Final	1.0.1	12/14/06	Added Appendix B to provide detail per SCI connection pair	Public

Editors

Chris Louden	Dave Silver	Treb Farrales
Andrew Chiu	Chris Broberg	Terry McBride
Chris Brown		

Table of Contents

Figures

Tables

1 Introduction

1.1 Background

On August 27, 2004, Homeland Security Presidential Directive-12 (HSPD-12) - "*Policy for a Common Identification Standard for Federal Employees and Contractors*" was issued. HSPD-12 directed the promulgation of a new Federal standard for a secure and reliable form of identification issued by all Federal agencies to their employees and contractors.

The HSPD-12 Implementation Executive Steering Committee (ESC) has requested establishment of several shared components with well-defined interfaces to assist agencies in meeting Personal Identity Verification (PIV) requirements. The HSPD-12 Implementation Architecture Working Group (AWG) convened under the auspices of the ESC to develop an architecture that defines shared component interfaces and interactions. The AWG based its work on analyses of PIV use cases.

The shared components provide agencies with a variety of options and resources to meet their HSPD-12 implementation requirements. An agency can implement a fully outsourced solution, leveraging shared components for every step in the process. In practice, many agencies will choose only the shared components they need, mixing shared and agency components to implement their overall HSPD-12 solution.

The shared component architecture supports, as necessary, Federal Information Processing Standard (FIPS) 201, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, as well as related documents such as National Institute of Standards and Technology (NIST) Special Publication 800-73, *Interfaces for Personal Verification* and NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*. In addition, the architecture does not affect standards or specifications tangentially encountered, such as the Electronic Fingerprint Transmission Specification (EFTS).

In addition, this document does not supersede or contradict any existing NIST publication, and should be used in conjunction with existing policies and procedures – particularly [NIST 800-79] and its guidelines for Federal agencies issuing, or preparing to issue, PIV cards that comply with FIPS 201 to their Federal employees and/or Federal contractor employees.

1.2 Authority

This document has been developed on behalf of The Office of Governmentwide Policy and the HSPD-12 Executive Steering Committee in furtherance of their charter to implement HSPD-12 from a “national” perspective.

1.3 Trust Model Overview

This document describes the Trust Model (TM) for the HSPD-12 shared component infrastructure (SCI). It captures assumptions the AWG has made on how architectural components will trust each other. This document assumes readers are familiar with the architectural concepts established by the AWG. Figure 1-1 shows the relationship amongst SCI documentation.

Figure 1-1 – SCI Documentation Hierarchy

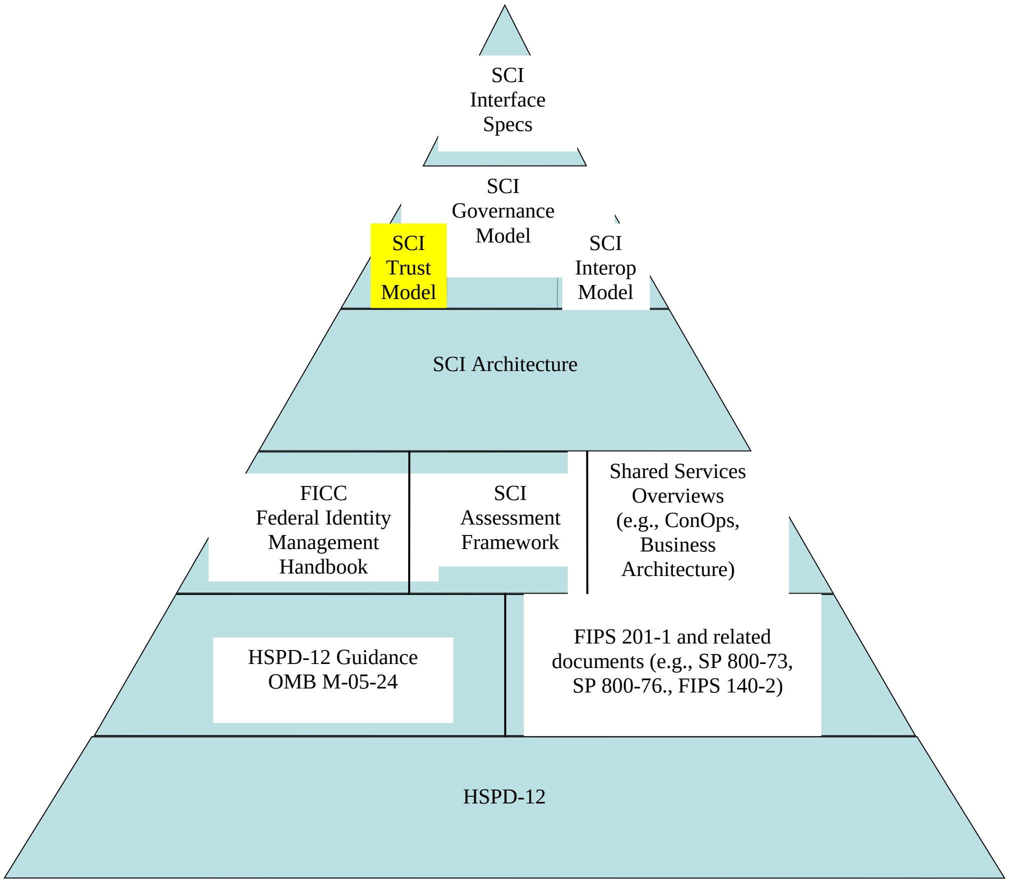

SCI Interface Specs
SCI Governance Model
SCI Trust Model
SCI Interop Model
SCI Architecture
FICC Federal Identity Management Handbook
SCI Assessment Framework
Shared Services Overviews (e.g., ConOps, Business Architecture)
HSPD-12 Guidance OMB M-05-24
FIPS 201-1 and related documents (e.g., SP 800-73, SP 800-76., FIPS 140-2)
HSPD-12

Figure 1-2 highlights the SCI TM. The SCI TM is limited in scope and its single purpose is to ensure that only those entities approved to participate in the SCI do so. In other words, it prevents non-approved entities from inserting themselves into any aspect of SCI processing. Before any technical interoperability occurs, and therefore any SCI processing (e.g., authorization, provisioning, System Infrastructure Provider (SIP) enrollment of enrollment stations, SCI transaction processing, transfer of data), an SCI component must ascertain that the entity "at the other end" is SCI-approved. This is always the first step in SCI technical interoperability. The SCI TM addresses the following SCI entities:

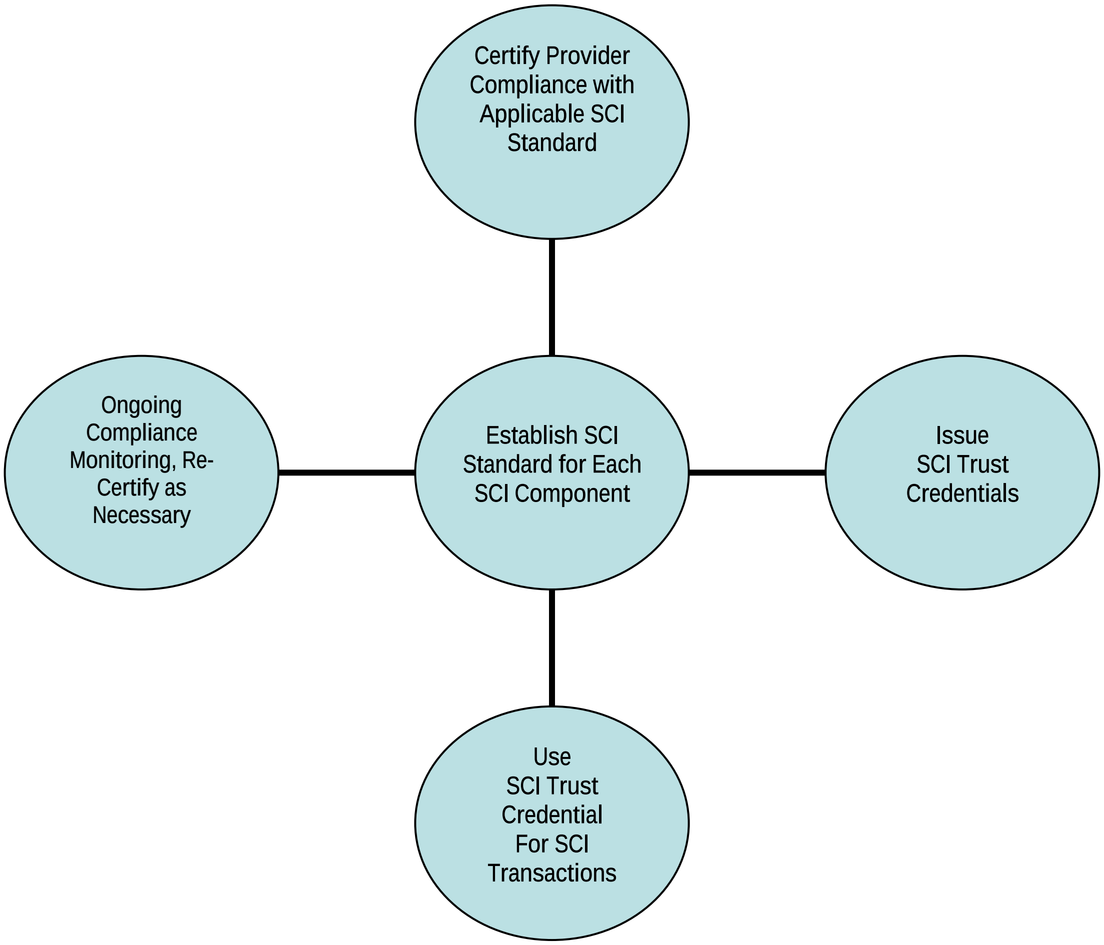
- **Shared components** – such as the Enrollment Service Provider (ESP), SIP, Production Service Provider (PSP), and Finalization Service Provider (FSP);
- **Agency systems** – such as an agency Human Resource (HR) system; and
- **Trusted Officers** – staff who operate shared components (e.g., an enrollment officer operating an ESP enrollment station).

Approved shared components and approved agency systems receive a SCI Trust Credential. The SCI Trust Credential has nothing to do with PIV cards and is not one of the credential types that can be loaded on to a PIV card. The SCI Trust Credential only authenticates a shared component or agency system as SCI-approved, thus able to interoperate with other SCI-approved entities. Approved SCI entities mutually exchange SCI Trust Credentials as the first step of SCI technical interoperability. Each SCI entity immediately validates the received SCI Trusted Credential. If both SCI Trust Credentials are valid, technical interoperability occurs. Otherwise, technical interoperability does not occur.

Trusted Officers must digitally sign work packages created at the shared component (e.g., at the enrollment station, at the finalization station). This must be done before a shared component transfers a work package to another entity (e.g., from an ESP to a SIP). The SCI Assessment Framework (see Section 2.1) requires processes to be in place that ensure only Trusted Officers have access to approved shared components and necessary certificates to digitally sign work packages. Note that the certificate issued to the Trusted Officer is not a SCI Trust Credential.

The SCI TM has nothing to do with PIV cards or the overall HSPD-12 processing that the SCI supports. The SCI TM is a subset of the SCI governance model.

Figure 1-2 – SCI Trust Model


Certify Provider Compliance with Applicable SCI Standard
Ongoing Compliance Monitoring, Re-Certify as Necessary
Establish SCI Standard for Each SCI Component
Issue SCI Trust Credentials
Use SCI Trust Credential For SCI Transactions

1.4 References

[FIPS 201] FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, March 2006.
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-v5.pdf

[HSPD-12] Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors;* August 27, 2004
http://csrc.ncsl.nist.gov/policies/Presidential-Directive-Hspd-12.html

[NIST 800-52] Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations
http://csrc.nist.gov/publications/nistpubs/800-52/SP800-52.pdf

[NIST 800-79] Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations
http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf

[NIST 800-95] Guide to Secure Web Services
http://csrc.nist.gov/publications/drafts/Draft-SP800-95.pdf

[SCI Architecture] HSPD-12 Shared Component Architecture
http://www.smart.gov/awg/documents/HSPD12sca.pdf

[SCI Interop Model] HSPD-12 Shared Component Infrastructure Technical Interoperability Model
http://www.smart.gov/awg/documents/SCItechnicalIOmodel.pdf

[SCI Metadata] HSPD-12 Shared Component Infrastructure Metatdata Management
http://www.smart.gov/awg/documents/SCImetadataManagement.pdf

[WS-Security] Web Services Security: SOAP Message Security 1.1 (WS-SECURITY 2004), OASIS Standard Specification, 1 February 2006
http://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf

2 Trust Model

For the Federal government to share resources and infrastructure there must be some basis for trust. Agencies that rely on architectural components provided by other organizations must be able to trust that those components have been established and operated in a trustworthy manner. Similarly, shared components must have a way of knowing they are dealing with a real, approved Trusted Officer. This section presents the model for establishing, verifying, and maintaining trust among components, and provides the tenets of the trust model.

2.1 SCI Assessment Framework

2.1.1 Establish Requirements for each SCI Component

Each SCI component (ESP, SIP, PSP, FSP, agency system) has a specific set of SCI requirements (i.e., qualifications) to which it must comply. Requirements are documented in Profiles, which are used by auditors during the SCI component certification phase. Each shared component has a dedicated Profile. Each Profile names and defines requirements that are appropriate for that SCI component. In addition, each Profile divides criteria into families of related requirements. Examples of requirement families include, but are not limited to the following:

- PIV Requirements;
- Personnel;
- Training;
- Physical security;
- Certified equipment;
- Certified software;
- Technical interoperability; and
- Ongoing operations.

2.1.2 Certify Provider Compliance with Requirements

An auditor or a SCI Governing Authority representative formally assesses the provider and its SCI component for compliance to the applicable Profile. The assessment may include an on-sight inspection, and the assessment auditor documents all findings. The SCI Governing Authority grants certification (i.e., approval to participate in the SCI) if the findings indicate full compliance and certification is in the best interest of the government.

In context of the SCI TM, the term “certification” applies only to the assessment of an SCI provider and its SCI component to determine compliance with the applicable Profile. Do not confuse the term with any other “review and determination” process (e.g., Federal Information Security Management Act (FISMA) Certification and Accreditation).

2.2 Issue SCI Trust Credentials

A dedicated SCI Governance Certification Authority (CA) issues SCI Trust Credentials to approved SCI components. Possession of this credential indicates compliance with SCI requirements, per the applicable Profile.

2.3 Use SCI Trust Credentials for Transactions

All SCI transactions require approved SCI components to exchange valid SCI Trust Credentials (i.e., mutual authentication). SCI components should not submit or accept SCI transactions if authentication fails. If an SCI component receives SCI transactions after authentication fails, the SCI transactions are not trusted (i.e., not processed).

2.4 Ongoing Compliance Monitoring

An auditor or SCI Governing Authority representative re-certifies approved SCI components at least every twenty-four (24) months. In addition, the approved SCI component provider must notify the SCI Governing Authority of any material change that may affect requirements compliance. The SCI provider must provide notification at least ninety (90) days prior to implementation. The SCI Governing Authority determines whether the changes require re-certification, in full or in part.

2.5 Security Principles

The SCI relies on a core set of security principles to protect program and transaction reliability, integrity, and privacy. Appendix B provides an overview on a per SCI connection basis.

SCI security principles are consistent with [NIST 800-95] in terms of:

- Addressing relevant web services security concepts (Table 2-1); and
- Using relevant security specifications (Table 2-2)

Table 2-1: SCI Mapping Against NIST 800-95 Security Concepts

NIST SP 800-95 Web Services Security Concept	SCI Approach
Authentication: Who is accessing the resource? Verify that principals (humans or application components) are who they claim to be through appropriate proof of identity. Determine the identity or role of a party attempting to perform some action, such as accessing a resource or participating in a transaction.	• Use of approved X.509 digital certificates (SCI Trust Certificates) issued by the government specifically for mutual authentication of SCI components prior to the exchange of transactions – no other certificates are permitted for this purpose. • SCI Trust Certificates issued by an FPKI OA operated Certification Authority dedicated exclusively to the HSPD-12 shared services initiative. • SCI Trust Certificates issued only after SCI certification. • Mutual authentication is via TLS (HTTPS), which is resistant to replay, sniffing, or other attacks. • Immediate validation of X.509 certificates presented for mutual authentication or digitally signing transactions using Certificate Revocation Lists (CRLs), and preferably Online Certificate Status Protocol (OCSP) or path-discovery/validation engines.
Authorization: What can they do? Grant permission for principals to access resources based upon access rights. Determine whether some party is allowed to perform a requested action or access particular resources, such as viewing a Web page, changing a password, or committing an organization to a ten million dollar transaction.	• SCI Assessment Framework, which certifies that SCI component providers have adequate processes in place to vet Trusted Officers, and control access to shared component services. • Trusted Officer's web browser certificate will include a Policy OID extension that the SIP uses as a technical control to determine legitimate user. The SIP then uses Access Control List for user access rights. • The SCI Governing Authority and Shared Component Providers will further define provisioning and authorization.
Integrity: Ensure that information is intact. Ensure that information is not changed in transit, either due to malicious intent or by accident. This may be information that is transmitted over a network, such as from a Web browser to a Web server, information stored in a database or file system, or information passed in a Web services message and processed by intermediaries.	• Message layer security per WS-Security (XML digital signatures): ▪ Trusted Officer digitally signs work package. ▪ SCI component digitally signs message and attachments prior to transmission

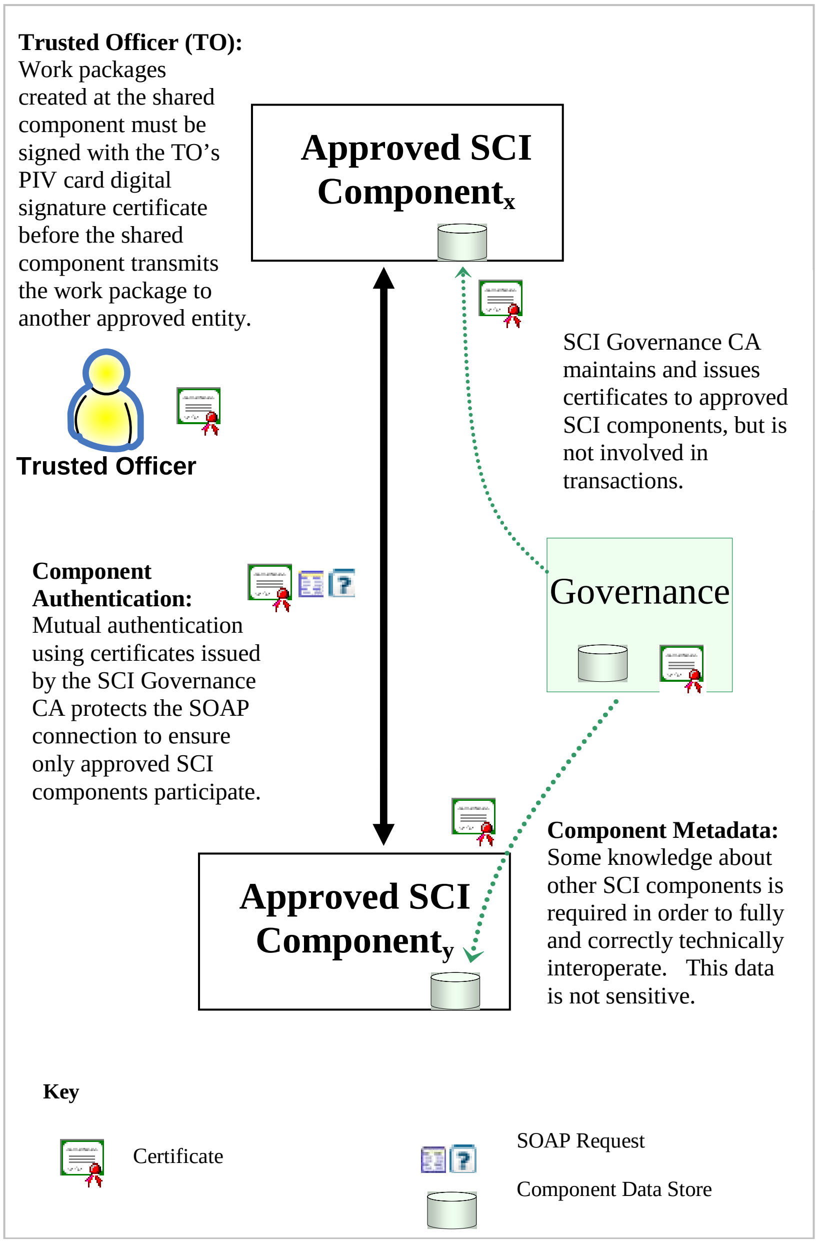
NIST SP 800-95 Web Services Security Concept	SCI Approach
Non-repudiation: Verify the identity of authors using electronic signatures analogous to handwritten signatures. Produce or verify an electronic signature intended to be the equivalent of a handwritten signature. Such a signature may be used for different purposes such as approval, confirmation of receipt, acceptance or agreement.	• Tight binding of transactions to initiators: ▪ Transaction header that includes unique Transaction ID, originating organization, originating system, and date/time stamp) ▪ Trusted Officer operating system component digitally signs work package ▪ SCI component digitally signs message and attachments prior to transmission
Confidentiality: Make content unreadable by unauthorized parties. Ensure that only legitimate parties may view content, even if other access control mechanisms are bypassed, and guarantee that exchanged information is protected against eavesdroppers. Confidentiality is generally associated with encryption technologies, although other approaches such as steganography (information hiding) might serve a similar purpose.	• Encryption of data in transport and at rest. • Message (and attachment) level encryption per WS-Security (XML Encryption, xenc:EncryptedKey approach). • Conformance of all encryption operations to FIPS specifications. ▪ FIPS certified cryptographic modules operated in FIPS mode • Transport Encryption by SSL with server certificate (non-mutual).
Privacy: Limit access and use of individually identifiable information.	• Only Trusted Officers (e.g., Enrollment Officer, Finalization Officer) see Personally Identifiable Information (PII), as necessary to perform duties. • No PII included in SCI email notifications (e.g., notification from SIP to agency points of contact).

Table 2-2: SCI Mapping Against NIST 800-95 Security Specifications

NIST SP 800-95 Security Dimension	**NIST SP 800-95 Security Requirement**	**NIST SP 800-95 Security Specification**	**SCI Approach**
Secure Messaging	Confidentiality and Integrity	WS-Security (XML Enc)	✓ **XML Encryption** **XML Digital Signature**
		SSL/TLS (HTTPS)	✓ **TLS per [NIST 800-52]**
	Authentication	WS-Security (SAML, X.509)	
		SSL/TLS (X.509)	✓ **TLS per [NIST 800-52]**
Resource Protection	Authorization	XACML	✓ **Access Control List for users accessing via Web Browser**
		XrML	
		RBAC, ABAC	
	Privacy	EPAL	To be addressed by SCI Governing Authority via the SCI Assessment Framework
		XACML	
	Accountability	Audit Tools, NIST 800-92	
Contract Negotiation	Registries	UDDI	To be addressed by SCI Governing Authority and SCI component providers
		ebXML	
	Semantic Discovery	SWSA	
		OWL-S	
	Business Contracts	ebXML	
Trust Management	Establishment	WS-Trust	
		XKMS	
		X.509	✓ **Mutual Authentication**
	Proxying	SAML	Proxying is Out of Scope
		WS-Trust	
	Federation	WS-Federation	Federation is Out of Scope
		Liberty IDFF	
		Shibboleth	
Security Properties	Policy	WS-Policy	To be addressed by SCI Governing Authority via the SCI Assessment Framework
	Security Policy	WS-SecurityPolicy	
	Availability	WS-ReliableMessaging	
		WS-Reliability	

Appendix A: Governance

The following diagram highlights the governance aspect of the trust model.



Trusted Officer (TO): Work packages created at the shared component must be signed with the TO's PIV card digital signature certificate before the shared component transmits the work package to another approved entity.

SCI Governance CA maintains and issues certificates to approved SCI components, but is not involved in transactions.

Component Authentication: Mutual authentication using certificates issued by the SCI Governance CA protects the SOAP connection to ensure only approved SCI components participate.

Component Metadata: Some knowledge about other SCI components is required in order to fully and correctly technically interoperate. This data is not sensitive.

Appendix B: SCI Connection Pair Summary

Connection Pair	Communication Summary	Message Level Digital Signature	Message Level Digital Encryption	Authentication (AuthN) Method B=Browser M=Machine	Certificates Involved
Agency-SIP	▪ SOAP/XML over HTTPS (TLS) ▪ SCA defined messages ▪ Also a SIP defined Web Interface for information look up (e.g., PIV cards delivered to finalization stations)	Agency ▪ XML digital signature per WS-Security SIP ▪ XML digital signature per WS-Security	Agency ▪ XML digital encryption (xenc:EncryptedKey) per WS-Security ▪ When PII ▪ Message & attachments SIP ▪ XML digital encryption (xenc:EncryptedKey) per WS-Security ▪ When PII ▪ Message & attachments	TLS Mutual AuthN (M-M) TLS Mutual AuthN (B-M)	Agency User of SIP Web Browser ▪ Any certificate to authN Browser ▪ The certificate includes a Policy OID extension that the SIP uses as a technical control to determine legitimate Agency User. The SIP then uses Access Control List for Agency User access rights. ▪ The SIP must import into its trust store the root certificates corresponding to Agency User certificates – to present correct hint list to the web browser Agency ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to encrypt messages ▪ SCI Trust Certificate to authN Agency SIP ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to encrypt messages ▪ SCI Trust Certificate to authN SIP

Connection Pair	Communication Summary	Message Level Digital Signature	Message Level Digital Encryption	Authentication (AuthN) Method B=Browser M=Machine	Certificates Involved
ESP-SIP	▪ SOAP/XML over HTTPS (TLS) ▪ SCA defined messages	Enrollment Officer (EO) ▪ Digitally signs enrollment package ▪ Enrollment station verifies EO signature before processing enrollment package message ▪ Enrollment station does not sign/send enrollment package if tampering discovered Enrollment Station ▪ XML digital signature per WS-Security SIP ▪ XML digital signature per WS-Security	Enrollment Station ▪ XML digital encryption (xenc:EncryptedKey) per WS-Security ▪ When PII ▪ Message & attachments SIP ▪ XML digital encryption (xenc:EncryptedKey) per WS-Security ▪ When PII ▪ Message & attachments	TLS Mutual AuthN (M-M)	Enrollment Officer ▪ Any certificate to sign enrollment package Enrollment Station ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to encrypt messages ▪ SCI Trust Certificate to authN station SIP ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to encrypt messages ▪ SCI Trust Certificate to authN SIP
SIP-PSP	▪ SOAP/XML over HTTPS (TLS) ▪ GlobalPlatform defined messages	PSP ▪ XML digital signature per WS-Security SIP ▪ XML digital signature per WS-Security	PSP ▪ XML digital encryption (xenc:EncryptedKey) per WS-Security ▪ When PII ▪ Message & attachments SIP ▪ XML digital encryption (xenc:EncryptedKey) per WS-Security ▪ When PII ▪ Message & attachments	TLS Mutual AuthN (M-M)	PSP ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to encrypt messages ▪ SCI Trust Certificate to authN PSP SIP ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to encrypt messages ▪ SCI Trust Certificate to authN SIP

Connection Pair	Communication Summary	Message Level Digital Signature	Message Level Digital Encryption	Authentication (AuthN) Method B=Browser M=Machine	Certificates Involved
SIP-FSP	▪ Finalization Officer-SIP communications via TLS-based web interface ▪ Card management commands (CMC) via secure channel that tunnels through web browser TLS connection ▪ Updating of PIV card located at FSP is via card type dependent software at the SIP (i.e., SIP selects software as needed per card type). ▪ Access to biometric reader located at FSP is through web browser TLS connection	Card reader at FSP ▪ Each CMC data packet is signed SIP ▪ Each CMC data packet is signed	Card reader at FSP ▪ Each CMC data packet is encrypted SIP ▪ Each CMC data packet is encrypted	TLS Mutual AuthN (B-M)	Finalization Officer ▪ Any certificate to authN Browser ▪ The certificate includes a Policy OID extension that the SIP uses as a technical control to determine legitimate FO. The SIP then uses Access Control List for FO access rights ▪ The SIP must import into its trust store the root certificates corresponding to FO certificates – to present correct hint list to the web browser SIP ▪ SCI Trust Certificate to sign CMC data packets ▪ SCI Trust Certificate to encrypt data packets ▪ SCI Trust Certificate to authN SIP ▪ The FSP must configure FO browsers with the SCI root certificate – to successfully validate server (SIP) authentication certificate

Connection Pair	Communication Summary	Message Level Digital Signature	Message Level Digital Encryption	Authentication (AuthN) Method B=Browser M=Machine	Certificates Involved
SIP-FPKI SSP	▪ Certificate Management Protocol (RFC4210) over HTTPS (TLS)	FPKI SSP ▪ Digital signature SIP ▪ Digital signature	No Encryption	TLS Mutual AuthN (M-M)[1]	FPKI SSP ▪ SCI Trust Certificate to authN FPKI SSP[2] ▪ SCI Trust Certificate to sign messages[3] ▪ Requires SIP to import all FPKI SSP root certificates into its trust store – to (a) authenticate FPKI SSP at TLS establishment, and (b) verify digital signature on FPKI SSP response messages SIP ▪ SCI Trust Certificate to sign messages ▪ SCI Trust Certificate to authN SIP ▪ Requires FPKI SSP to import SCI root certificate into its trust store – to verify digital signature on SIP request messages

[1] If FPKI SSP is not capable of mutual authentication, server-side (FPKI SSP) authentication will be done, as is done today.
[2] If FPKI SSP is not capable of using SCI issued certificate, FPKI SSP will use other certificate to authenticate itself, as is currently done.
[3] If FPKI SSP is not capable of using SCI issued certificate, FPKI SSP will use other certificate to sign, as is currently done.

Appendix C: Glossary and Acronyms

Term	Description
Certification	Assessment and determination of compliance to applicable requirements. For SCI purposes, the certification regards SCI requirements only, and is unrelated to FISMA Certification and Accreditation.
Certification Authority	A trusted entity that issues and revokes public key certificates. More specifically, a CA is an authority in a network that issues and manages security credentials and public keys for message encryption. As part of a public key infrastructure (PKI), a CA checks with a registration authority (RA) to verify information provided by the requestor of a digital certificate. If the RA verifies the requestor's information, the CA can then issue a certificate.
Component	Sub-system within the SCI that performs a well defined set of functionality and clearly specified interactions and interrelationships.
Credential	Digital documents used in electronic authentication that bind an identity or an attribute to a subscriber's token. Electronic credentials serve the same purpose as traditional paper credentials such as passports, birth certificates, and driver licenses – they attest to the identity or other attributes of an individual or entity.
Governance (SCI Governance)	Governance comprises the organizations, policies, processes and systems that control, direct, and oversee the SCI in a comprehensive and authoritative manner. Governance ensures ongoing SCI consistency, reliability, and trustworthiness, which are the basis of agency reliance on SCI components. Examples of governance include (1) determining which SCI components can participate, and under what conditions, (2) approving issuance of credentials, (3) metadata management, and (4) SCI provider/component certification. Comprehensive SCI governance protects the best interests of the Federal government and HSPD-12.
Governing Authority (SCI Governing Authority)	The organization responsible for comprehensive SCI governance. The Governing Authority facilitates development of SCI governance policies, processes, and systems.
Hypertext Transfer Protocol, Secure (HTTPS)	The protocol for accessing a secure Web server. Using HTTPS in the URL instead of HTTP directs the message to a secure port number rather than the default Web port number of 80. The session is then managed by a security protocol such as Secure Socket Layer (SSL).

Term	Description
Metadata	Information necessary for SCI components (e.g., ESP, SIP, PSP, FSP, agency system) to technically interoperate. An SCI component must be configured with metadata. Failure to completely and correctly configure metadata can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of SCI components. The Governing Authority maintains an authoritative copy of metadata, and distributes it to SCI providers who must use the metadata to configure their SCI components before operating. Metatadata is not sensitive information and is not expected to change very often.
Online Certificate Status Protocol (OCSP)	On-line, real-time protocol used to determine the status of a public key certificate. OCSP overcomes the chief limitation of CRL: that updates must be frequently dowloaded to keep the client-side list current. When a user attempts to access a server, OCSP sends a request for certificate status information. The server sends back a response of "current", "expired," or "unknown."
Path Validation and Discovery (PDVal)	Path discovery (also called path building) is the process of locating all of the intermediate certificates and certificate revocation lists (CRLs) needed to validate an end entity certificate (e.g., the end user's public key certificate) or determining that no valid certification path exists. Path validation is the process of verifying the discovered chain of certificates. Verification checks each certificate in the path for a variety of factors relevant to trust, including, but not limited to: • Verifying the digital signature on each certificate in the discovered path • Verifying that each certificate in the discovered path has not been revoked • Verifying that each certificate in the discovered path has not expired • Verifying that each certificate in the discovered path has a compatible assurance level PDVal is used to validate a public key certificate. It is a method for finding a trusted chain of certificates from an AA's trust anchor, through the FPKI, to the end user's issuing CA. It is the E-Authentication Initiative recommended approach because it simplifies management of the AA and improves security by allowing the AA to leverage the FPKI, rather than using a manual configuration process to replicate the security and policy information embedded in cross-certificates. Path building is complex and can lead to many interesting problems in complex PKIs. Two primary alternatives are the Trusted List model found in browsers, and online certificate validation services. The former relies on distribution of all trust anchors to all systems. The latter provides an external service.

Term	Description
	Certificate path validation procedures are based on the algorithm supplied in ITU-T Recommendation X.509 and further defined in Internet Engineering Task Force (IETF) Request for Comments (RFC) 3280. Certificate path processing verifies the binding between the subject distinguished name and/or subject alternative name and the subject public key defined in the target certificate. The binding is limited by constraints, which are specified in the certificates that comprise the path, and inputs that are specified by the relying party. To ensure secure interoperation of PKI-enabled applications, the path validation must be done in accordance with the X.509 and RFC 3280 specifications.
Requirement	A characteristic that a system must possess in order to be acceptable.
Secure Socket Layer (SSL)	Protocol for transmitting private documents via the Internet by using a private key to encrypt data that's transferred over the SSL connection.
SOAP	Lightweight XML-based messaging protocol used to encode the information in Web service request and response messages before sending them over a network. It consists of three parts: an envelope that defines a framework for describing what is in a message and how to process it, a set of encoding rules for expressing instances of application-defined data types, and a convention for representing remote procedure calls and responses. SOAP messages are independent of any operating system or protocol and may be transported using a variety of Internet protocols, including MIME and HTTP.
Standards	Mandatory conventions and practices.
Technical Interoperability	Technical interoperability is the coordinated implementation of systems to support electronic communication and data exchange between those systems.
Transport Layer Security (TLS)	TLS is a protocol created to provide authentication, confidentiality and data integrity between two communicating applications. TLS is based on a precursor protocol called “The Secure Sockets Layer Version 3.0” (SSL 3.0) and is considered to be an improvement to SSL 3.0. TLS is defined by [RFC 2246] and [RFC 3546]. TLS is effectively SSL version 3.1.
Trust	Confidence in other components based on proven compliance with standards, as evidenced by the possession of a valid SCI credential.
WS-Security	Standard that addresses data exchange security as part of a Web service. Specifically, WS-Security is a mechanism for adding security information into SOAP messages. SOAP provides a flexible technique for structuring messages, but it does not directly address how to secure the messages.

Acronym	Abbreviation For
ABAC	Attribute Based Access Control
AWG	Architecture Working Group
CA	Certification Authority
CRL	Certificate Revocation List
EbXML	Electronic Business Extensible Markup Language
EFTS	Electronic Fingerprint Transmission Specification
EPAL	Enterprise Privacy Authorization Language
ESC	Executive Steering Committee
ESP	Enrollment Service Provider
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FPKI OA	Federal Public Key Infrastructure Operational Authority
FSP	Finalization Service Provider
HR	Human Resource
HSPD-12	Homeland Security Presidential Directive-12
HTTPS	Hypertext Transfer Protocol, Secure
IDFF	Identity Federation Framework
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OWL-S	Web Ontology Language for Web Services
PII	Personally Identifiable Information
PIV	Personal Identity Verification
PSP	Production Service Provider
RBAC	Role Based Access Control
SAML	Security Assertion Markup Language
SCI	Shared Component Infrastructure
SIP	System Infrastructure Provider
SSL	Secure Socket Layer
SWSA	Semantic Web Services Architecture
TLS	Transport Layer Security
TM	Trust Model
TO	Trusted officer
UDDI	Universal Description, Discovery, and Integration
XACML	Extensible Access Control markup Language
XKMS	XML Key Management Service
XML	Extensible Markup Language
XrML	Extensible Rights Markup Language
WS	Web Services