HSPD-12 Shared Component Infrastructure Metadata Management

Version 1.0.0

February 7, 2007

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.0	06/02/06	Document creation	Enspier
Draft	0.0.1	06/05/06	Updates based on internal comments	Enspier
Draft	0.0.2	06/06/06	Updates based on internal comments	Enspier
Draft	0.0.3	06/06/06	Updates based on internal comments	Enspier
Draft	0.0.4	06/06/06	Updates based on internal comments	Enspier
Draft	0.0.5	09/29/06	Updates based on internal comments	Enspier
Draft	0.0.6	09/30/06	Updates based on internal comments	AWG
Draft	0.0.7	11/15/06	Updates per AWG comments	AWG
Draft	0.0.8	11/23/06	Updates per AWG comments	AWG
Draft	0.0.9	12/8/06	Updates per AWG comments	AWG
Draft	0.0.10	12/13/06	Updates per final internal review	Enspier
Draft	0.1.0	12/15/06	Released for public review	Public
Final	1.0.0	2/7/07		Public

Editors

Treb Farrales	David Silver	Andrew Chiu
Terry McBride	Glenn Ballard	Rick Uhrig

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).

Components are deployed in an operational HSPD-12 shared component infrastructure (SCI). SCI components technically interoperate with each other, as appropriate, and include:

- **Shared Components (Shared Services**) – various services shared government-wide:
  - *Enrollment Station Provider (ESP)* – identity proofs applicants in accordance with FIPS 201 standards and I-9 documentation and captures biometrics, including picture and 10-slap fingerprints.
  - *Systems Infrastructure Provider (SIP)* – manages full lifecycle of the PIV card via Identity Management System (IDMS) and Card Management System (CMS) functionality.
  - *Production Service Provider (PSP)* – produces and personalizes PIV cards.
  - *Finalization Service Provider (FSP)* – finalizes personalization of PIV cards and completes issuance to the applicant.
- **Agency Components (Agency Systems)** – systems used by a single agency (i.e., not shared). An example of an agency system is:
  - An agency Human Resource (HR)/Personnel system.

SCI Providers build and operate SCI components.

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 References

[Agency-SIP] Agency to System Infrastructure Provider Interface Specification
http://www.smart.gov/awg/documents/AgencytoSIPinterfaceSpec.pdf

[ESP-SIP] Enrollment Service Provider to Systems Infrastructure Provider Interface Specification
http://www.smart.gov/awg/documents/ESPtoSIPinterfaceSpec.pdf

[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

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

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

[SCI Trust] HSPD-12 Shared Component Infrastructure Trust Model
http://www.smart.gov/awg/documents/SCItrustModel.pdf

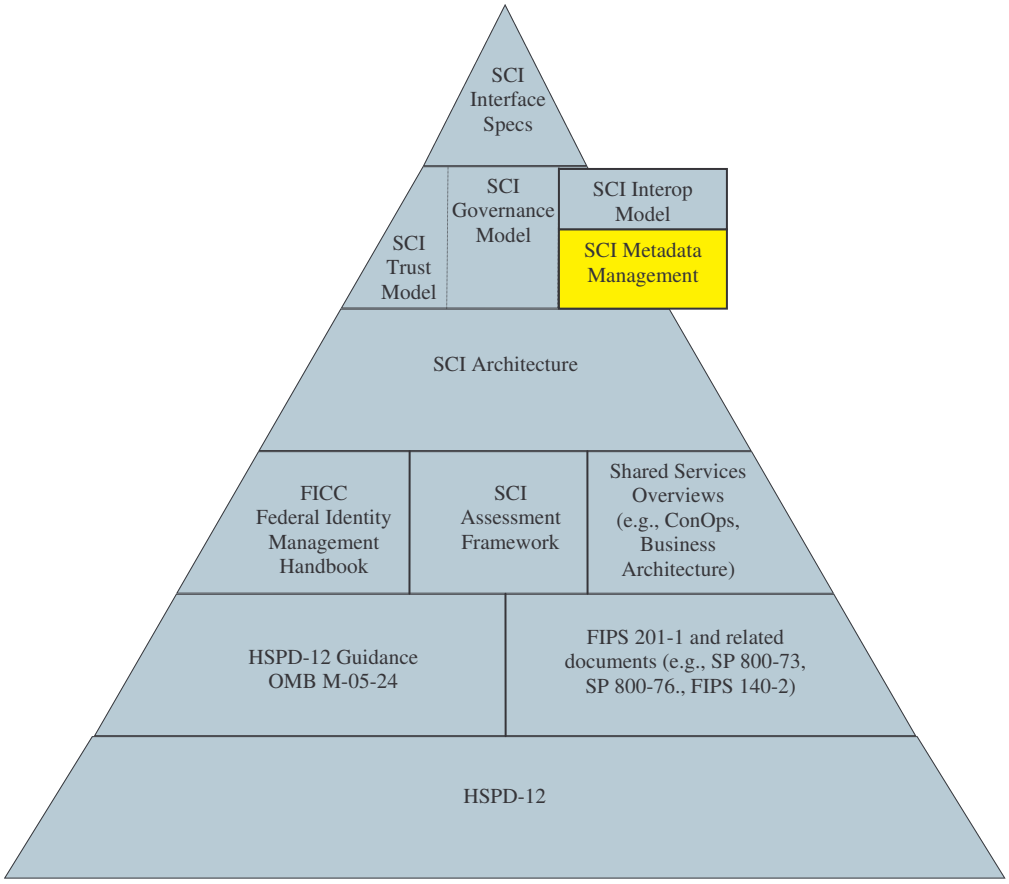
[SIP-PSP] Systems Infrastructure Provider to Production Systems Provider Interface Specification
http://www.smart.gov/awg/documents/SIPtoPSPinterfaceSpec.pdf

[SIP-FPKISSP] Systems Infrastructure Provider to FPKI Shared Service Provider Interface Specification
http://www.smart.gov/awg/documents/SIPtoFPKISSPinterfaceSpec.pdf

1.4 Metadata Management Overview

This document describes SCI metadata management. It captures assumptions the Architecture Working Group (AWG) has made about the full lifecycle of SCI metatdata (definition, distribution, configuration, use, and maintenance). 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



Every SCI component (ESP, SIP, PSP, FSP, FPKI SSP, Agency System) requires certain information about each SCI component with which it will interoperate – in advance of interoperating. For example, an agency system that interoperates with a specific SIP cannot do so unless it knows, in advance, the web service provider URL of that SIP.

Metadata is the means of describing and conveying such information. An SCI provider creates and maintains a metadata file for each SCI component it operates. There is one metadata file per SCI component. Metadata files are exchanged amongst SCI providers so that each SCI component can be configured with the metadata information of each SCI component with which it will interoperate. For

example, a PSP that interoperates with four (4) different SIPs needs the metadata file for each one of those SIPs. However, another PSP that interoperates with only one (1) SIP will need the metadata file for just that one SIP.

Not all metadata is configured into an SCI component for use at run-time. Some metadata items are informational to the SCI provider, so that the SCI provider can make certain determinations and/or decisions. For example, an SCI provider looks at the metadata item that specifies the interface version of the SCI component with which its SCI component will interoperate. The SCI provider then determines whether its SCI component can interoperate using that interface version, or a supported backward-compatible version. Another example is metadata data items that provide the SCI provider (and Governing Authority) with contact information for the SCI provider who owns the SCI component described by the metadata file. This allows the SCI provider (or Governing Authority) to contact that SCI provider if there are any issues or questions.

Use of metadata is in addition to implementing applicable SCI interface specifications. Metadata derives from two sources: (a) SCI providers describing their SCI components, and (b) the Governing Authority assigning unique values to certain metadata items.

The Governing Authority maintains an authoritative copy of everyone's metadata, and distributes metadata files to SCI providers as applicable. SCI providers must use the applicable metadata to configure their SCI components before operating. Failure to configure metadata completely and correctly can preclude technical interoperation, or result in unexpected consequences or negative impacts to any number of SCI components.

SCI metadata is not sensitive and is unlikely to change often. SCI metadata does not pertain to [FIPS 201]. The sole purpose of SCI metadata is to facilitate technical interoperation amongst SCI components. SCI metadata management is a subset of the SCI Interoperability Model.

2 SCI Metadata

SCI Providers must describe each of their SCI components via metadata. The SCI Providers then exchange their metadata to applicable other SCI providers. The set of metadata required to describe an SCI component depends upon the SCI component.

Table 2-1 describes the full set of metadata elements and attributes. An element is a logical grouping of information. Attributes are specific information items that comprise an element. SCI Providers select elements from this list as necessary to describe their SCI components. The presentation approach used here does not imply a particular description or implementation method. The SCI governing authority decides how metadata is described (e.g., XML), as well as published and discovered (e.g., manually, automated via UDDI) – in the initial term, and over time as circumstances warrant. In addition, the SCI governing authority decides final rules pertaining to formats and valid values.

Some SCI components implement one or more web services. For each web service, an SCI Provider may publish and support more than one version concurrently. This precludes the need for immediate migration to a newer version, which can be operationally disruptive and high-risk. Accordingly, SCI metadata supports multiple listings of the same web service, qualified by version number. A web service consumer simply uses the metadata of the web service version appropriate for it.

This document uses the following cardinality terms:

- **Mandatory Once** – must appear exactly once
- **Mandatory Repeating** – must appear at least once and may appear an indeterminate number of times.
- **Optional Repeating** – may appear an indeterminate number of times.

Figure 2-1: Suite of Metadata Elements and Attributes

Row #	Element	Attributes	Information Specified By	Notes
1	SCI Component Information	SCI Component Type	SCI Provider	Example: Agency System, ESP, SIP, PSP, FPKI SSP
		SCI Component ID	SCI Governing Authority	Unique SCI component identifier Format to be determined by Governing Authority
2	SCI Provider Information	SCI Provider Name	SCI Provider	Entity operating the SCI component
		SCI Provider Contact Name		Full name of primary contact
		SCI Provider Contact Phone		Telephone number of primary contact
		SCI Provider Contact Email		Email address of primary contact
3	Preferred FPKI SSP Information	FPKI Provider Name	Agency	Name of the FPKI SSP to use for an agency
		FPKI SCI Component ID		SCI ID of the FPKI SSP to use for an agency
4	FPKI SSP Service	Service URL	FPKI SSP	Example: https://123.ssp.com/v1.0.0/FPKIService
		Service Version		Example: 1.0.0
5	Agency Service Information	Web Service URL	SIP	Example: https://123.abc.com/v1.0.0/WebService
		Web Service Version		Example: 1.0.0
6	Enrollment Service Information	Web Service URL	SIP	Example: https://123.abc.com/v1.0.0/WebService
		Web Service Version		Example: 1.0.0
7	Card Production Service Information	Web Service URL	PSP	Example: https://123.abc.com/v1.0.0/WebService
		Web Service Version		Example: 1.0.0
8	PSP Response Service Information	Web Service URL	SIP	Example: https://123.abc.com/v1.0.0/WebService
		Web Service Version		Example: 1.0.0

Row #	Element	Attributes	Information Specified By	Notes
9	Component Certificate Information	Machine Certificate	SCI Provider (from applicable CA)	Certificate issued to SCI component. Format: -----BEGIN CERTIFICATE----- [Entire Certificate] -----END CERTIFICATE-----
		Certificate Purpose		Example: Authentication, Digital Signing, Digital Encryption
10	User Certificate Information	User Certificate	SCI Provider (from applicable CA)	Certificates issued to agency operators and Finalization Officers to access SCI components via a web interface. Format: -----BEGIN CERTIFICATE----- [Entire Certificate] -----END CERTIFICATE-----
11	Root Certificate Information	Root Certificate	SCI Provider (from applicable CA)	Certificate of CA that issues a user certificate (see item #10 above). Root certificates are necessary to build and present the correct "hint list" in an SCI web browser (e.g., SIP-Agency web browser, SIP-FSP web browser). Format: -----BEGIN CERTIFICATE----- [Entire Certificate] -----END CERTIFICATE-----

2.1 Agency System

2.1.1 Agency Metadata File

An agency must use metadata to describe each agency system participating in the SCI. This includes using information from the applicable FPKI SSP metadata file to specify which FPKI SSP the SIP must use on behalf of the agency. Table 2-1 summarizes the agency system metadata file.

Table 2-1: Agency System Metadata File

Row #	Required Metadata Elements	Cardinality	Document Cross-Reference	Notes
1	SCI Component Information	Mandatory Once		
2	SCI Provider Information	Mandatory Once		
3	Preferred FPKI SSP Information	Mandatory Once	[SIP-FPKISSP]	
4	Component Certificate Information	Mandatory Repeating	[SCI Trust]	▪ Certificate(s) issued to the Agency System for authentication
5	User Certificate Information	Optional Repeating	[SCI Trust]	▪ List each certificate that will be used by an agency operator in an SCI component web browser ▪ Users are presumed to be provisioned in the SCI component they are trying to access via the web interface
6	Root Certificate Information	Optional Repeating	[SCI Trust]	▪ Required if User Certificate Information is included ▪ Repeat as many times as necessary to ensure every user certificate has a corresponding root certificate

2.1.2 Agency System Metadata Configuration

An agency system must be configured with metadata from each SCI component with which it technically interoperates. Table 2-2 summarizes what metadata information must be configured by the agency system.

Table 2-2: Metadata configured into an Agency System

Row #	SCI Component Providing Information	Information to Configure into the Agency System
1	SIP	Component Certificate Information
		Agency Service Information

In addition, the agency should configure its system with the SCI Trust CA root certificate for purposes of validating a Component Certificate presented by a SIP.

2.2 SIP Metadata File

2.2.1 SIP Metadata File

A SIP must use metadata to describe itself. Table 2-3 summarizes the SIP metadata file.

Table 2-3: SIP Metadata File

Row #	Required Metadata Elements	Cardinality	Document Cross-Reference	Notes
1	SCI Component Information	Mandatory Once		
2	SCI Provider Information	Mandatory Once		
3	Agency Service Information	Mandatory Repeating	[Agency-SIP]	
4	Enrollment Service Information	Mandatory Repeating	[ESP-SIP]	
5	PSP Response Service Information	Mandatory Repeating	[SIP-PSP]	
6	Component Certificate Information	Mandatory Repeating	[SCI Trust]	▪ Certificate(s) issued to the SIP

2.2.2 SIP Metadata Configuration

A SIP must be configured with metadata from each SCI component with which it technically interoperates. Table 2-4 summarizes what metadata information must be configured by the SIP.

Table 2-4: Metadata configured into a SIP

Row #	SCI Component Providing Information	Information to Configure into the SIP
1	Agency System	Component Certificate Information
		User Certificate Information
		Root Certificate Information
		Preferred FPKI SSP Information
2	ESP Enrollment Station	Component Certificate Information
3	PSP	Component Certificate Information
		Card Production Service Information
4	FSP	User Certificate Information
		Root Certificate Information
5	FPKI SSP	Component Certificate Information

In addition, the SIP should configure its system with the SCI Trust CA root certificate for purposes of validating Component Certificate(s) presented by an agency system, enrollment station, or PSP.

2.3 ESP Enrollment Station Metadata File

2.3.1 Enrollment Station Metadata File

An ESP must use metadata to describe each enrollment station participating in the SCI. Table 2-5 summarizes the ESP enrollment station metadata file.

Table 2-5: ESP Enrollment Station Metadata File

Row #	Required Metadata Elements	Cardinality	Document Cross-Reference	Notes
1	SCI Component Information	Mandatory Once		
2	SCI Provider Information	Mandatory Once		
3	Component Certificate Information	Mandatory Repeating	[SCI Trust]	▪ Certificate(s) issued to the Enrollment Station

2.3.2 Enrollment Station Metadata Configuration

An ESP enrollment station must be configured with metadata for each SCI component with which it technically interoperates. Table 2-6 summarizes what metadata information must be configured by the enrollment station.

Table 2-6: Metadata configured into an Enrollment Station

Row #	SCI Component Providing Information	Information to Configure into the Enrollment Station
1	SIP	Component Certificate Information
		Enrollment Service Information

In addition, the ESP should configure each enrollment station with the SCI Trust CA root certificate for purposes of validating Component Certificate(s) presented by a SIP.

2.4 PSP Metadata File

2.4.1 PSP Metadata File

A PSP must use metadata to describe itself. Table 2-7 summarizes the PSP metadata file.

Table 2-7: PSP Metadata File

Row #	Metadata Item	Cardinality	Document Cross-Reference	Notes
1	SCI Component Information	Mandatory Once		
2	SCI Provider Information	Mandatory Once		
3	Card Production Service Information	Mandatory Repeating	[SIP-PSP]	
4	Component Certificate Information	Mandatory Repeating	[SCI Trust]	▪ Certificate(s) issued to the PSP

2.4.2 PSP Metadata Configuration

A PSP must be configured with metadata from each SCI component with which it technically interoperates. Table 2-8 summarizes what metadata information must be configured by the PSP.

Table 2-8: Metadata configured into a PSP

Row #	SCI Component Providing Information	Information to Configure into the PSP
1	SIP	Component Certificate Information
		PSP Response Service Information

In addition, the PSP should configure its system with the SCI Trust CA root certificate for purposes of validating Component Certificate(s) presented by a SIP.

2.5 FSP Finalization Station Metadata

2.5.1 Finalization Station Metadata File

An FSP must use metadata to describe every enrollment station participating in the SCI. Table 2-9 summarizes the FSP finalization station metadata file.

Table 2-9: ESP Enrollment Station Metadata File

Row #	Required Metadata Elements	Cardinality	Document Cross-Reference	Notes
1	SCI Component Information	Mandatory Once		
2	SCI Provider Information	Mandatory Once		
3	User Certificate Information	Optional Repeating	[SCI Trust]	▪ Repeat for each certificate that will be used by a Finalization Officer in an SCI component web browser ▪ Users are presumed to be provisioned in the SCI component they are trying to access via the web interface
4	Root Certificate Information	Optional Repeating	[SCI Trust]	▪ Required if User Certificate Information is included ▪ Repeat as many times as necessary to ensure every user certificate has a corresponding root certificate

2.5.2 Finalization Station Metadata Configuration

The FSP should configure Finalization Officer web browsers with the SCI Trust CA root certificate for purposes of validating the Component Certificate presented by a SIP during web browser processing.

2.6 FPKI SSP Metadata

2.6.1 FPKI SSP System Metadata File

A FPKI SSP must use metadata to describe itself. Table 2-10 summarizes the FPKI SSP metadata file.

Table 2-10: FPKI SSP Metadata File

Row #	Required Metadata Elements	Cardinality	Document Cross-Reference	Notes
1	SCI Component Information	Mandatory Once		
2	SCI Provider Information	Mandatory Once		
3	FPKI SSP Service	Mandatory Repeating	[SIP-FPKISSP]	
4	Component Certificate Information	Mandatory Repeating	[SCI Trust]	▪ Certificate(s) issued to the FPKI SSP

2.6.2 FPKI SSP Metadata Configuration

A FPKI SSP system must be configured with metadata for each SCI component with which it technically interoperates. Table 2-11 summarizes what metadata information must be configured by the FPKI SSP.

Table 2-11: Metadata configured into a FPKI SSP

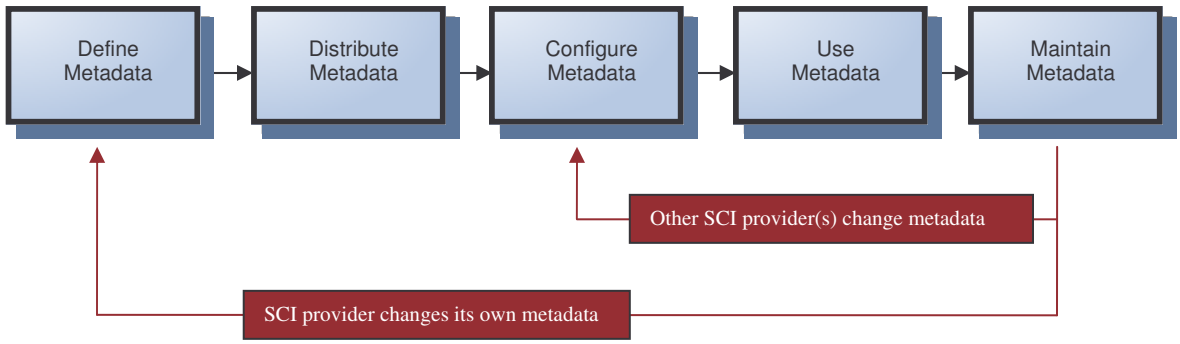
Row #	SCI Component Providing Information	Information to Configure into the FPKI SSP System
1	SIP	Component Certificate Information

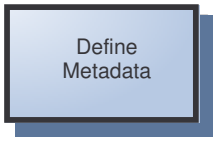
In addition, the FPKI SSP should configure its system with the SCI Trust CA root certificate for purposes of validating the Component Certificate(s) presented by a SIP.

3 Metadata Management Lifecycle

The metadata management lifecycle includes five (5) distinct phases. The Governing Authority defines the specific guidelines and operational details of each phase. This document is limited to describing each metadata management phase at a high level, solely to convey the basic concept and general sequence of events. Figure 3-1 highlights the full lifecycle of metadata management within the HSPD-12 SCI.

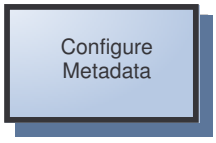
Figure 3-1: SCI Component Metadata Management Model/Life Cycle



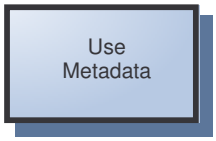


The SCI provider creates a metadata file for a specific SCI component. All metadata entries applicable to that SCI component are added. The SCI provider verifies that all the entries are present, and their values are complete and correct. Values entered derive from the SCI provider itself, or from the Governing Authority. Initially, it is likely the Governing Authority will deliver Governing Authority -provided values via a non-automated, out-of-band-process. This phase supports maintenance updates, whereby the SCI provider simply updates the already exiting metadata file as necessary.

The SCI provider gives the Governing Authority a copy of the newly created or updated metadata file. Once received, the Governing Authority maintains the authoritative copy of the metadata file. The Governing Authority is the clearinghouse for all authoritative metadata. On an ongoing basis, as circumstances warrant, the Governing Authority provides each SCI provider with the set of metadata files applicable to each SCI component the SCI provider operates. Initially, it is likely that metadata distribution will be a manual process. As the SCI scales sufficiently upward over time, the Governing Authority is likely to implement an automated distribution process.



Upon receiving all metadata files applicable to a specific SCI component, the SCI provider updates that SCI component with the relevant information from the metadata files received. As a result, the SCI component has information that it may use at run-time. How configuration is accomplished is outside the scope of this document, and may differ from one SCI component to another.



At run time, an SCI component uses the information of other SCI components configured into it for various technical interoperation purposes. One example is determining where to go to connect to another SCI component. An agency system, for example, determines it needs to interoperate with a specific SIP. The agency system uses that SIP's unique SCI Component ID to find that SIP's set of information previously configured into it. The agency system then finds the information specifying that SIP's web service URL for agency subscribers. Another example is SCI component mutual authentication - the exchange and validation of SCI Trust Certificates, which is a security handshake preceding technical interoperation. An SCI component finds the SCI Trust Certificate of the other SCI component previously configured into it. The SCI component then validates the certificate it finds for the other SCI component.

SCI providers maintain their operational SCI components with respect to metadata – in a diligent and timely manner. This ensures ongoing, correct technical interoperation, especially when metadata information changes. Maintenance pertains to (a) an SCI provider updating and redistributing a metadata file for any of its SCI components, and (b) an SCI provider re-configuring its SCI component(s) when it receives new or updated metadata files of other SCI providers (via the Governing Authority).

Appendix A: Acronyms and Definitions

Term	Description
Agency system	Systems used by a single agency (i.e., not shared), but technically interoperate with other SCI components. An example of an agency system is a Human Resource (HR)/Personnel system.
Enrollment Service Provider (ESP)	ESPs provide local presence for enrollment of applicants using enrollment stations. Enrollment stations identity proof applicants in accordance with FIPS 201 standards and I-9 documentation, and capture biometrics including picture and 10-slap fingerprints. The information captured is used for (1) background investigations, and (2) printing information on the PIV card.
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.
Federal Public Key Infrastructure Shared Service Provider (FPKI SSP)	Properly qualified provider of PKI services for the government .
Finalization Service Provider (FSP)	FSPs provide local presence to finalize personalization of the cards and complete issuance to the applicant. The same organization that handles ESP operations for an agency may also manage FSP operations.
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 SCI 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.
Production Service Provider (PSP)	PSPs produce and personalize PIV cards.
SCI Component	An ESP, SIP, PSP, FSP, Agency System, FPKI SSP

Term	Description
SCI Provider	SCI providers build, deliver, and operate components. For shared components, the provider can be a commercial entity or an agency – in either case, the provider makes their component(s) available for use government wide. For agency components, the provider is the agency itself, and the components (e.g., HR system) likely already exist and simply need enhancement to interoperate with the appropriate shared component.
Systems Infrastructure Provider (SIP)	SIPs provide the software functionality required to manage PIV credentials. SIPs build, host, and operate software that provides agencies with critical IDMS and Card Management System (CMS) functionality.

Acronym	Abbreviation For
AWG	Architecture Working Group
CA	Certification Authority
EFTS	Electronic Fingerprint Transmission Specification
ESC	Executive Steering Committee
ESP	Enrollment Service Provider
FIPS	Federal Information Processing Standards
FPKI SSP	Federal Public Key Infrastructure Shared Service Provider
FSP	Finalization Service Provider
HSPD-12	Homeland Security Presidential Directive 12
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PIV	Personal Identity Verification
PSP	Production Service Provider
SCI	Shared Component Infrastructure
SIP	Systems Infrastructure Provider
UDDI	Universal Description, Discovery & Integration
XML	Extensible Markup Language