HSPD-12 Shared Component Infrastructure Technical Interoperability Model

Version 1.0.0

November 12, 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		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 and further internal review	Enspier
Draft	0.0.5	08/21/06	Revised per AWG review	AWG
Draft	0.0.6	08/30/06	Made editorial changes.	Enspier
Draft	0.1.0	08/31/06	Released for public review.	Public
Draft	0.1.1	09/30/06	Updated per public comments, AWG guidance, and further internal review	AGW
Final	1.0.0	09/12/06	Final Version	Public

Editors

Chris Louden	Dave Silver	Treb Farrales
Chris Broberg		

Table of Contents

Figures

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.

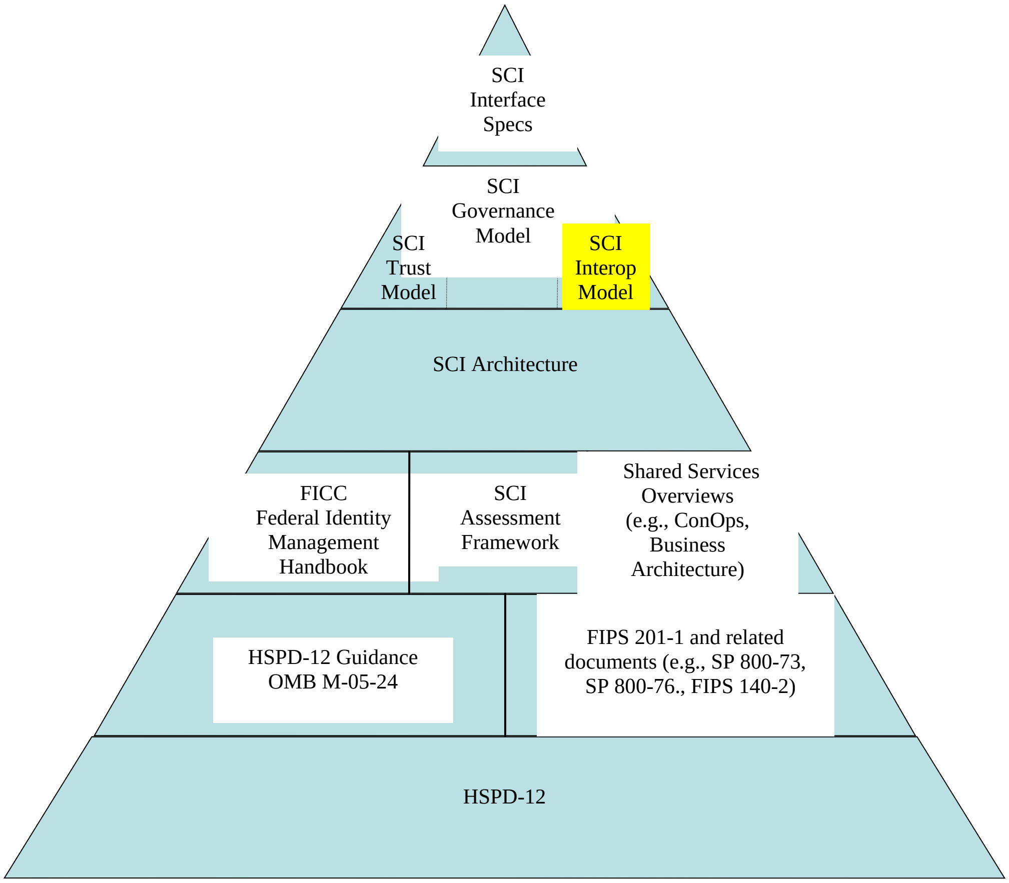
1.2 Authority

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 Technical Interoperability Model Overview

This document describes the Technical Interoperability Model (TIM) for the HSPD-12 shared component infrastructure (SCI). It captures assumptions the AWG has made on how architectural components will technically interoperate with 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

1.4 Scope

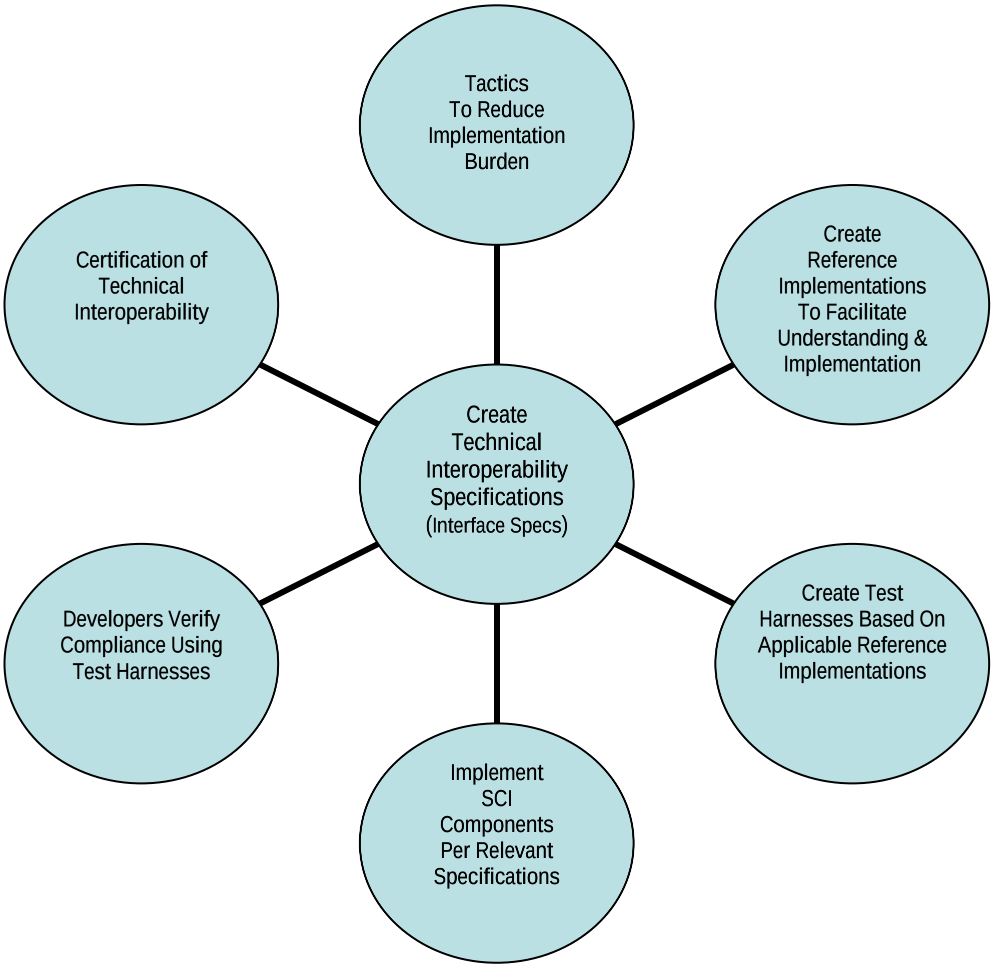
Figure 1-2 highlights the various aspects of the SCI TIM. The SCI TIM is limited in scope and its single purpose is to ensure all SCI components (e.g., Enrollment Service Provider (ESP), System Infrastructure Provider (SIP), Production Service Provider (PSP), Finalization Service Provider (FSP), agency systems) technically interoperate in a robust, reliable, consistent manner, in accordance with [FIPS 201] and related documents. To achieve this, the SCI TIM:

- Defines an appropriate technical interoperability specification for each SCI component; and
- Determines whether each SCI component, offered by a provider for use in the SCI, complies with all applicable technical interoperability specifications.

To be integrated into the SCI production environment, an SCI component must prove full compliance with applicable technical interoperability specifications.

The SCI TIM has nothing to do with PIV card technical interoperability within a PIV system (e.g., between a PIV card and a Physical Access Control System (PACS), between a PIV card and a Logical Access Control System (LACS). The SCI TIM pertains only to technical interoperation between SCI components in support of HSPD-12 PIV card deployment and life cycle management. The SCI TIM is a subset of the SCI governance model.

Figure 1-2 –SCI Technical Interoperability Model


Tactics To Reduce Implementation Burden
Certification of Technical Interoperability
Create Reference Implementations To Facilitate Understanding & Implementation
Create Technical Interoperability Specifications (Interface Specs)
Developers Verify Compliance Using Test Harnesses
Create Test Harnesses Based On Applicable Reference Implementations
Implement SCI Components Per Relevant Specifications

1.5 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

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

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

2 Interoperability Model

For SCI components to technically interoperate successfully and correctly, a comprehensive model (i.e., strategy) is required. This section presents the model for establishing, verifying, and maintaining technical interoperability among SCI components and provides the tenets of the SCI TIM. The model facilitates a repeatable, consistent, provable approach. In doing so, agencies that rely on SCI components can be sure that the transactions they depend upon execute in a timely, reliable, consistent manner.

2.1 Create Technical Interoperability Specifications

The AWG defines and fully documents a complete technical interoperability specification (i.e., interface specification) for each SCI component. Each specification provides sufficient detail to allow for independent SCI component development. That is, each SCI provider implements its SCI component without dependency on the implementation status and timetable of other SCI components. SCI providers only need to implement their SCI component in accordance with applicable specifications. To reduce the implementation burden, various tactics are used. This includes, but is not limited to:

- Building on existing standards;
- Simplifying the number of options/branches as much as possible;
- Minimizing the number of transaction parameters; and
- Returning informative transaction return codes.

Reducing burden likely reduces implementation risk, time and cost.

Agency systems that interoperate with SCI shared services (e.g., an agency Human Resource (HR) system that interoperates with the SIP) must do so via the applicable SCI interface specifications.

2.2 Create Reference Implementations

The SCI Governing Authority oversees the creation of one reference implementation per shared component. Each reference implementation created:

- Illustrates the intentions of the interface specification;
- Verifies the interface specification can indeed be implemented;
- Reveals any difficulties with the interface specification; and
- Provides examples for implementers of that shared component.

Reference implementations may include software code, libraries, modules, and objects that SCI component implementers can leverage. These will be available on a reference implementation case-by-case basis. Where and when possible, actual implementations will be used as the basis of reference implementations.

Reference implementations facilitate understanding and thus more complete and correct implementation of SCI components per applicable specifications. This facilitates more reliable, consistent SCI component implementations, which reduces risk and increases confidence in the transactions relied upon.

2.3 Create Test Harness

A test harness is created for each SCI component interface specification and is based on applicable reference implementations. Test harnesses facilitate compliance with applicable SCI technical interoperability specifications by allowing SCI component implementers to check compliance during the development lifecycle.

Using test harnesses facilitates more fully compliant SCI components from the onset, thus reducing overall deployment timeframes because of fewer non-compliance issues.

2.4 Implement According to Specifications

SCI component providers implement their SCI components in accordance with applicable SCI technical interoperability specifications. SCI providers use applicable reference implementations to (1) ensure full understanding of all applicable specifications, (2) leverage software artifacts, and (3) correctly implement specifications. During implementation, and upon concluding implementation, SCI component providers use applicable test harnesses to verify compliance to all applicable SCI technical interoperability specifications.

2.5 Certification of Technical Interoperability

Prior to operational deployment, certifiers test the SCI component to ensure correct and reliable technical interoperation, per applicable SCI specifications. The SCI Governing Authority certifies each SCI component's technical interoperability using applicable test harnesses.

In context of the TIM, "certification" applies only to the assessment of SCI technical interoperability and determination of compliance to applicable TIM interoperability specifications. The term should not be confused with any other review and determination process, such as the Federal Information Security Management Act (FISMA) Certification and Accreditation (C&A).

Appendix A: Glossary and Acronyms

Term	Description
Certification	Assessment and determination of compliance to applicable standards. For SCI purposes, certification pertains to verification of SCI components. It does not pertain to other certification requirements such as FISMA C&A.
Component	Sub-system within the SCI that performs a well defined set of functionality and clearly specified interactions and interrelationships.
Governance	Governance comprises the processes and systems by which the Managed Service Office asserts its authority to determine which SCI components can participate, and under what conditions. Governance includes (1) Issuance of credentials, (2) Management of Metadata, (3) SCI provider/component certification. See [SCI Governance] for more information.
Reference Implementation	A software example of a standard. A standard is much easier to understand with a working example in hand. The purpose of a reference implementation is generally to increase awareness and familiarization of the specification within the development community. A reference implementation is, in general, an implementation of a specification to be used as a definitive interpretation for that specification. At least one relatively trusted implementation of each interface is necessary to (1) discover errors or ambiguities in the specification, and (2) validate the correct functioning of the test suite.
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.
Test Harness	Collection of software tools and test data configured to test a program unit by running it under varying conditions and monitor its behavior and outputs. It has two main parts namely, Test execution engine and the test script repository.

Acronym	Abbreviation For
AWG	Architecture Working Group
C&A	Certification and Accreditation
EFTS	Electronic Fingerprint Transmission Specification
ESC	Executive Steering Committee
ESP	Enrollment Service Provider
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FSP	Finalization Service Provider
HR	Human Resource
HSPD-12	Homeland Security Presidential Directive-12
LACS	Logical Access Control System
NIST	National Institute of Standards and Technology
PACS	Physical Access Control System
PIV	Personal Identity Verification
PSP	Production Service Provider
SCI	Shared Component Infrastructure
SIP	System Infrastructure Provider
TIM	Technical Interoperability Model