Finalization Service Provider to System Infrastructure Provider Interface

Version 1.0.0

February 7, 2007

Document History

Status	Release	Date	Comment	Audience
Draft	0.0.0	12/07/06	Initial Template	AWG
Draft	0.0.1	12/08/06	Initial Content added	AWG
Draft	0.1.0	12/15/06	Released for public review	Public
Final	V1.0.0	2/7/07		Public

Editors

Joe Broghammer
Peter Cox
Brian Kelly
Chris Louden
Dave Silver
Owen Unangst
Chris Broberg
Glenn Ballard
Treb Farrales
Mike Janiszewski
Eric Mitchell
Judith Spencer
Terry McBride
Poornima Koka
Andrew Chiu
Larry Fobian
Steve Lazerowich
Eric Olsson
Eric Stout
Matt Tebo
Chris Brown

Table of Contents

1 Introduction

This document describes Finalization Service Provider (FSP) and Systems Infrastructure Provider (SIP) data exchange. One should read [SCI Architecture] before reading this document.

1.1 Authority

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

1.2 References

[FIPS 201] FIPS PUB 201-1 Change Notice 1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006
http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf

[GP Card Spec] GlobalPlatform Card Specification, Version 2.2, March 2006
http://www.globalplatform.org/specificationview.asp?id=card

[NIST 800-73] NIST Special Publication 800-73-1 Interfaces for Personal Identity Verification, March 2006
http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf

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

[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

[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 FSP to SIP Interfaces

Finalization is initiated by the Finalization Officer (FO). Once initiated, the SIP manages and controls the majority of finalization processing – the notable exception is setting a PIN on the PIV card, which the applicant does using a PINpad. In general, the FSP's role is to provide a physical location for finalization to occur, a browser to access SIP web pages, and network connectivity to the PIV card via a smart card reader attached to an FSP computer.

2.1 XML Interfaces

No Extensible Markup Language (XML) messages are exchanged between the FSP and SIP. Accordingly, no XML interfaces are defined for this connection pair.

2.2 Web Interfaces

The FSP provides a browser for the FO to access SIP web pages for (a) FO authentication, (b) applicant identification, and (c) initiation of PIV card finalization. These web pages are an important interface between the SIP and the FO. The web interface connection is via Hypertext Transport Protocol, Secure (HTTPS).

The SIP-provided web interface for finalization is outside the scope of this document. SIP vendors will design and implement the finalization web interface as befits their product.

2.3 Card Edge Interfaces

The Shared Component Architecture (SCA) does not specify a standard card edge interface for finalization. The following sections address (a) why defining a finalization card edge interface is appropriate in the long-term, (b) cannot be achieved in the near-term, and (c) the approach for converging in the future toward a standard finalization card edge interface.

2.3.1 Need for a Standard Finalization Card Edge Interface

Much of finalization involves issuing commands directly to the PIV card for loading data and generating keys. These commands are physically transmitted through a secure channel that tunnels through the web browser TLS connection, on to and through the smart card reader at the finalization station. For finalization interface purposes, there are two key considerations:

1. The commands used are directly supported by the PIV card, and are understood at the *card edge*. These are often called *card edge commands*, and the interface is often called a *card edge interface*.

2. The SIP, not the FSP, issues these commands. Even though the PIV card, applicant, FO and FSP are all geographically at the Finalization Station, it is the SIP that invokes the card edge commands to finalize the PIV card.

Accordingly, the card edge command set used during finalization should be considered a critical interface component and is appropriately addressed in an interface specification.

2.3.2 Barriers to a Standard Finalization Card Edge Interface

The commands and data formats for accessing PIV card information during operational use are well defined and standardized in [NIST 800-73]. While these interfaces are sufficient for card use, they do not include everything needed for PIV card lifecycle maintenance, including PIV card finalization.

The Government considered expanding [NIST 800-73] interfaces to also include PIV card maintenance. However, this approach was not taken. As a result, there are no standard interfaces required for PIV card lifecycle maintenance; and PIV card vendors are on their own regarding the finalization card edge.

At least eight (8) different PIV card Applications appear on the NIST PIV Program Validation List at http://csrc.nist.gov/npivp/. Each is certified to adhere to [NIST 800-73] for operational use. However, each also supports additional proprietary card edge commands needed for finalization and other lifecycle management activities. Further, since the validated products come from three (3) significantly different types of smart card technology – Javacard, MULTOS, and file system –the complexity of standardizing the finalization card edge is significantly increased.

Within the SCA, this variation is currently accommodated by the Card Management System (CMS) component within the SIP. The CMS drives finalization., using specific knowledge of each PIV card's proprietary finalization card edge.

2.3.3 Approach to a Standard Finalization Card Edge Interface

The recommended approach for realizing a standard card edge interface for PIV card finalization is widespread adoption and implementation of [GP Card Spec] in validated PIV card products.

[GP Card Spec] defines a standard card edge for lifecycle management that includes most or all the commands required for PIV card finalization. However, this is a relatively recent specification (March 2006), so it will be some time before its functionality is fully implemented, widely adopted, and available in validated PIV card products.

Appendix A: Glossary & Acronyms

Term	Description
Applicant	Individual seeking a PIV card.
Extensible Markup Language (XML)	Specification developed by the W3C. XML is a pared-down version of SGML, designed especially for Web documents. It allows designers to create their own customized tags, enabling the definition, transmission, validation, and interpretation of data between applications and between organizations.
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.
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).
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
FIPS	Federal Information Processing Standards
FO	Finalization Officer
FSP	Finalization Service Provider
HSPD-12	Homeland Security Presidential Directive-12
HTTPS	Hypertext Transfer Protocol Secure
NIST	National Institute of Standards and Technology
PIN	Personal Identification Number
PIV	Personal Identity Verification
SCA	Shared Component Architecture
SCI	Shared Component Infrastructure
SIP	System Infrastructure Provider
XML	Extensible Markup Language