NIST Special Publication 800-73-2
2nd DRAFT

Interfaces for Personal Identity Verification – Part 4: The PIV Transitional Interface and Data Model Specification

National Institute of Standards and Technology
U.S. Department of Commerce

James F. Dray
Scott B. Guthery
Hildegard Ferraiolo
William I. MacGregor
Ramaswamy Chandramouli

I N F O R M A T I O N S E C U R I T Y

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD, 20899-8930

March 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
Dr. James Turner, Acting Director

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Draft Special Publication 800-73-2, Part 4, 16 pages, (March 2008)

Acknowledgements

The authors (James Dray, Hildegard Ferraiolo, William MacGregor and Ramaswamy Chandramouli of NIST and Scott Guthery of Mobile Mind Inc) wish to thank their colleagues who reviewed drafts of this document and contributed to its development. Special thanks to the Government Smart Card Interagency Advisory Board (GSC-IAB) and InterNational Committee for Information Technology Standards (INCITS) for providing detailed technical inputs to the SP 800-73 development process. Special recognition is due to Booz Allen Hamilton, and particularly to Ketan Mehta, who made essential technical and editorial contributions. The authors also gratefully acknowledge and appreciate the many contributions from the public and private sectors whose thoughtful and constructive comments improved the quality and usefulness of this publication.

Table of Contents

List of Appendices

List of Tables

1. Introduction

The Homeland Security Presidential Directive HSPD-12 called for a common identification standard to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201 (FIPS 201) [1] was developed to establish standards for identity credentials. Special Publication 800-73 (SP 800-73) specifies interface requirements for retrieving and using the identity credentials from the PIV Card[1] and is a companion document to FIPS 201.

1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This recommendation is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This recommendation has been prepared for use by federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright though attribution is desirable. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the Office of Management and Budget (OMB), or any other Federal official.

1.2 Purpose

FIPS 201 defines procedures for the PIV lifecycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201 also specifies that the identity credentials must be stored on a smart card. SP 800-73 contains technical specifications to interface with the smart card to retrieve and use the identity credentials. The specifications reflect the design goals of interoperability and PIV Card functions. The goals are addressed by specifying a PIV data model, card edge interface, and application programming interface. Moreover, SP 800-73 enumerates requirements where the standards include options and branches. The specifications go further by constraining implementers' interpretation of the normative standards. Such restrictions are designed to ease implementation, facilitate interoperability, and ensure performance, in a manner tailored for PIV applications.

[1] A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, biometric data) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

1.3 Scope

SP 800-73 specifies the PIV data model, Application Programming Interface (API) and card interface requirements necessary to comply with the use cases, as defined in Section 6 of FIPS 201 and further elaborated in Appendix B of SP 800-73 Part 1. Interoperability is defined as the use of PIV identity credentials such that client-application programs, compliant card applications, and compliant integrated circuits cards (ICC) can be used interchangeable by all information processing system across Federal agencies.

Part 2, 3 and 4 of SP 800-73 describes two realizations of the client application programming and card command interfaces for personal identity verification: the transitional interfaces (this Part 4) and the end-point interfaces (Part 2 and 3). The transitional interface may be used by agencies with an existing identity card program as an optional intermediate step in evolving to the end-point interfaces.

This fourth part, Special Publication 800-73 (SP 800-73) Part 4 *The PIV Transitional Interfaces and Data Model Specification* contains informative links to specifications of the transitional PIV card command interface and client application programming interface of the transitional PIV card. Part 4 also describes the PIV Data Model that is common between End-Point and transitional interface specifications.

1.4 Audience and Assumptions

This document is targeted at Federal agencies and implementers of PIV systems. Readers are assumed to have a working knowledge of smart card standards and applications.

1.5 Document Overview and Structure

All sections in this document are *normative* (i.e., mandatory for compliance) unless specified as *informative* (i.e., non-mandatory). Following is the structure of this document:

Part 4 is organized as follows:

+ Section 1, *Introduction*, provides the purpose, scope, audience, and assumptions of the document and outlines its structure.
+ Section 2: *Common Data Model and Migration Considerations* provides the specification for that which is common to both the transitional and end-point interfaces. Section 2 also includes guidance as to strategies for migrating from the transitional interfaces to the end-point interfaces.
+ Section 3: *The Transitional Interfaces* provides links to transitional interface specification that are implemented today by agencies with legacy GSC-IS based card deployments. This section is informative.
+ Appendix A, *Terms, Acronyms, and Notation*, contains the list of Terms and Acronyms used in this document and explains notation in use. This section is informative.
+ Appendix B, *References*, contains the list of documents used as references by this document.

2. Overview and Migration Considerations

2.1 Migration Considerations

SP 800-73 Parts 1 - 4 provide two interface specifications: 1) a transitional Card Specification as described in this Part 4; and 2) a FIPS 201 End-Point Card Specification as described in Parts 1- 3 of SP 800-73. Part 4 interface specifications are informative PIV profile derived from the Government Smart Card Interoperability Specification (GSC-IS), Version 2.1. [2] It presents one possible path that agencies with existing GSC-IS based smart card deployments may choose to follow during the transition to End-Point PIV card deployment. All agencies must ultimately comply with End-Point Specifications in accordance with the schedule provided by the Office of Management and Budget (OMB). End-Point deployment is therefore the end state of each agency's transition plan.

Agencies may either elect to implement an approved transitional specification as specified in this document (Part 4), particularly when migrating from currently widely implemented identity card architectures to the End-Point specifications described in Parts 1- 3 of SP 800-73, or to implement the Part 4 specifications directly. NIST supports agency efforts towards government-wide PIV-End-Point interoperability described in the Parts 1 - 3 specification. NIST also supports transition specifications of Part 4 for widely implemented deployments as they migrate towards the End-Point specifications.

The migration path to End-Point implementation is based on continuity of the PIV data model. Exactly the same data appear on both the transitional and end-point interfaces. Therefore, description of the data for personal identity verification, the PIV data model, is duplicated from the Part 1 (Section 3) in Section 2.2 below[2].

Specific considerations associated with this migration path are highlighted below:

+ The transitional specifications present a subset of the dual GSC-IS card edge interfaces. The End-Point specifications present a unified card edge interface that is technology independent and compliant with existing international standards.

+ The End-Point specifications provide limited credential administration functionality. A unified and interoperable card management solution between issuing domains including the loading of new card applications is not provided.

+ Named data objects within the data model may be directly accessed. If a data object is managed by the default application, it can be retrieved directly without selecting the application. This avoids a requirement to search through discovery to get named data objects. Otherwise, the (non-default) application managing the data object is selected and the data object is retrieved from this application. The GET DATA command described in Part 2 retrieves a data object in one command.

+ The data model including the data model namespace is controlled by NIST and hence change management of well known and interoperable data objects will be managed by NIST in the process of managing the overall data model. As a first step in

[2]Although the same data objects are present on the end-point and transitional interfaces, different representations for the same data objects may be used.

namespace management, the data object identifiers of GSC-IS and transitional systems in the range '0000' through '9FFF' will be explicitly managed by NIST and data object identifiers of GSC-IS and transitional systems in the range 'A000' through 'FFFF' are placed under control of the card issuer.

+ Each application managing one or more of the directly addressable data model data objects will have a version number enabling the relying application to determine the level of the information contained within the object. The version of the End-Point PIV Card Application is encoded in its full Application IDentifier (AID) which is returned when this application is selected. This is in addition to the Card Capability Container (CCC) style data model naming facility carried over from GSC-IS.

+ Agency-specific applications can be included on cards containing PIV applications. These applications may define and manage their own namespaces that are used when the application is used. Such applications will have application identifiers outside the application namespace managed by NIST; that is, application identifiers not rooted on the NIST Registered application provider IDentifier (RID).

2.2 PIV Data Model

Table 1 defines a high level view of the data model. Each on-card storage container is labeled either as Mandatory (M) or Optional (O). This data model is designed to enable and support dual interface cards. Note that access conditions based on the interface mode (contact vs. contactless) take precedence over all Access Rules defined in Table 1, Column 3.

Table 1. Data Model Containers

Container Name	ContainerID	Access Rule for Read	Contact / Contactless[3]	M/O
Card Capability Container	0xDB00	Always	Contact	Mandatory
CHUID Buffer	0x3000	Always	Contact and Contactless	Mandatory
PIV Authentication Certificate Buffer	0x0101	Always	Contact	Mandatory
Fingerprint Buffer	0x6010	PIN	Contact	Mandatory
Printed Information Buffer	0x3001	PIN	Contact	Optional
Facial Image Buffer	0x6030	PIN	Contact	Optional
Digital Signature Certificate Buffer	0x0100	Always	Contact	Optional
Key Management Certificate Buffer	0x0102	Always	Contact	Optional
Card Authentication Certificate Buffer	0x0500	Always	Contact and Contactless	Optional
Security Object Buffer	0x9000	Always	Contact	Mandatory

[3] Contact interface mode means the container is accessible through contact interface only. Contact and contactless interface mode means the container can be access from either interface.

Appendix A, Part 1 provides a detailed spreadsheet for the data model. ContainerIDs and Tags within the containers are defined by this data model and in accord with SP 800-73 Part 1 naming conventions.

A PIV Card Application shall contain five mandatory interoperable data objects and may contain five optional interoperable data objects. The five mandatory data objects for interoperable use are as follows:

+ Card Capability Container
+ Card Holder Unique Identifier
+ X.509 Certificate for PIV Authentication
+ Card Holder Fingerprints
+ Security Object

The five optional data objects for interoperable use are as follows:

+ Card Holder Facial Image
+ Printed Information
+ X.509 Certificate for Digital Signature
+ X.509 Certificate for Key Management
+ X.509 Certificate for Card Authentication

2.3 Mandatory Data Elements

The five mandatory data objects support FIPS 201 minimum mandatory compliance.

2.3.1 Card Capability Container

The CCC is mandatory for compliance with the Government Smart Card Interoperability Specification (GSC-IS) [3] specification. It supports minimum capabilities for retrieval of data model and application information.

The data model of the PIV Card Application shall be identified by data model number “0x10”. Deployed applications use “0x00” through “0x04”. This enables the GSC-IS application domain to correctly identify a new data model name space and structure as defined in this document.

2.3.2 X.509 Certificate for PIV Authentication

The X.509 Certificate and its associate private key, as defined in FIPS 201, is used to authenticate the card and cardholder. Private key operations with the PIV Authentication Key requires the Personal Identification Number (PIN).

2.3.3 Card Holder Unique Identifier

The Card Holder Unique Identifier (CHUID) data object is defined in accordance with the Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS). [4] For this specification, the CHUID is common between the contact and contactless chips. For dual chip implementations, the CHUID is copied in its entirety between the two chips.

In addition to the requirements specified in TIG SCEPACS, the CHUID on a PIV Card shall meet the following requirements:

+ The Buffer Length field is an optional TLV element. This element is the length in bytes of the entire CHUID, excluding the Buffer Length element itself, but including the CHUID's Asymmetric Signature element. The calculation of the asymmetric signature must exclude the Buffer Length element if it is present.

+ The Federal Agency Smart Credential Number (FASC-N) shall be consistent with the TIG SCEPACS Option for "System Code || Credential Number" to establish a credential number space of 9,999,999,999 credentials. The same FASC-N value shall be used in all the PIV data objects that include the FASC-N. The value of the Credential Series (CS) field in the FASC-N shall be 1. It is recommended that the value of the Personal Identifier (PI) field in the FASC-N be 0000000000 (i.e., ten BCD digits, each representing zero) to minimize the disclosure of permanent individual identifiers.

+ The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros. The GUID is included to enable future migration away from the FASC-N into a robust numbering scheme for all issued credentials.

+ The DUNS and Organizational Code fields are optional.

+ The Authentication Key Map[4] is specified as an optional field which enables the application to discover the key reference.

+ The Expiration Date is mapped to the reserved for future use (RFU) tag 0x35, keeping that within the existing scope of the TIG SCEPACS specification. This field shall be 8 bytes in length and shall be encoded as YYYYMMDD.

+ The CHUID is signed in accordance with FIPS 201. The card issuer's digital signature key shall be used to sign the CHUID and the associated certificate should be placed in the signature field of the CHUID.

2.3.4 Card Holder Fingerprints

The fingerprint data object specifies the primary and secondary fingerprints in accordance with the FIPS 201. The Common Biometric Exchange Formats Framework (CBEFF) headers shall contain the FASC-N and shall require the Integrity Option. The headers shall not require the Confidentiality Option.

[4] The Authentication Key Map is deprecated. It will be eliminated in a future revision of SP 800-73.

2.3.5 Security Object

The Security Object is in accordance with Appendix C of PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1. [5] Tag "0xBA" is used to map the ContainerIDs in the PIV data model to the 16 Data Groups specified in the Machine Readable Travel Document (MRTD). The mapping enables the Security Object to be fully compliant for future activities with identity documents.

The "DG-number-to-Container-ID" mapping object TLV in tag "0xBA"encapsulates a series of three byte triples - one for each PIV data object included in the Security Object. The first byte is the Data Group (DG) number, and the second and third bytes are the most and least significant bytes (respectively) of the Container ID value. The DG number assignment is arbitrary; however, the same number assignment applies to the DataGroupNumber(s) in the DataGroupHash(es). This will ensure that the ContainerIDs in the mapping object refers to the correct hash value in the Security Object (0xBB).

The 0xBB Security Object is formatted according to the MRTD document's Appendix C. The LDS Security Object itself must be in ASN.1 DER format, formatted as specified in Appendix C.2. This structure is then inserted into the encapContentInfo field of the CMS object specified in Appendix C.1.

The card issuer's digital signature key used to sign the CHUID shall also be used to sign the Security Object. The signature field of the Security Object, Tag "0xBB" shall omit the issuer's certificate, since it is included in the CHUID. Unsigned data elements such as the Printed Information data object shall be included in the Security Object[5] if present.

2.4 Optional Data Elements

The five optional data elements of FIPS 201, when implemented, shall conform to the specifications provided in this document.

2.4.1 Printed Information Data Object

All FIPS 201 mandatory information printed on the card is duplicated on the chip in this data object. The Security Object enforces integrity of this information according to the issuer. This provides specific protection that the card information must match the printed information, mitigating alteration risks on the printed media.

2.4.2 Facial Image Data Object

The photo on the chip supports human verification only. It is not intended to support facial recognition systems for automated identity verification.

2.4.3 X.509 Certificate for Digital Signature

The X.509 Certificate and its associate private key, as defined in FIPS 201, supports the use of digital signatures for the purpose of document signing. The Public Key Infrastructure (PKI) cryptographic function is protected with a "PIN Always" access rule. In other words, PIN must be submitted every time immediately before the *Digital Signature Key* operation. This ensures cardholder participation every time the private key is used for digital signature generation.

[5]For ease of data object updates, signed PIV data elements may be excluded from the Security Object.

2.4.4 X.509 Certificate for Key Management

The X.509 Certificate and its associate private key, as defined in FIPS 201, supports the use of encryption for the purpose of confidentiality. This key pair is escrowed by the issuer for key recovery purposes. The PKI cryptographic function is protected with a "PIN" access rule. In other words, once the PIN is submitted subsequent *Key Management Key* operations can be performed without requiring PIN again. This requires cardholder activation, but enables multiple compute operations without additional cardholder consent.

2.4.5 X.509 Certificate for Card Authentication

This key and certificate (if the key is an asymmetric key) supports device to device card authentication. Cardholder consent is not required to use this key. The access rule for PKI cryptographic functions is "Always" meaning the key can be used always without access control restrictions.

3. Transition Card Interfaces

3.1 Middleware Application Programming Interface

Reference [7] is an example of a transitional (GSC-IS) middleware API specification.

3.2 Card Edge Commands

Reference [8] is an example of a transitional (GSC-IS) card edge command specification.

Appendix A—Terms, Acronyms, and Notation

A.1 Terms

Card	An integrated circuit card.
Card Application	A set of data objects and card commands that can be selected using an application identifier.
Data Object	An item of information seen at the card command interface for which are specified a name, a description of logical content, a format and a coding.

A.2 Acronyms

APDU	Application Protocol Data Unit
BSI	Basic Services Interface
CBEFF	Common Biometric Exchange Formats Framework
CCC	Card Capability Container
CHUID	Card Holder Unique IDentifier
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
GSC-IAB	Government Smart Card Interagency Advisory Board
GSC-IS	Government Smart Card Interoperability Specification
GUID	Global Unique Identification Number
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
ISO	International Standards Organization
LSB	Least Significant Bit
MRTD	Machine Readable Travel Document
MSB	Most Significant Bit
OMB	Office of Management and Budget

PACS	Physical Access Control System
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
RFU	Reserved for Future Use
RID	Registered application provider IDentifier
RSA	Rivest, Shamir, Aldeman
SP	Special Publication
TIG	Technical Implementation Guidance
VM	Virtual Machine

A.3 Notation

The sixteen hexadecimal digits shall be denoted using the alphanumeric characters 0, 1, 2…, A, B, C, D, E, and F. A byte consists of two hexadecimal digits, for example, ‘2D’. A sequence of bytes may be enclosed in single quotation marks, for example 'A0 00 00 01 16' rather than given as a sequence of individual bytes, 'A0’ ‘00’ ‘00’ ‘01’ ‘16'.

A byte can also be represented by bits b8 to b1, where b8 is the most significant bit (MSB) and b1 is the least significant bit (LSB) of the byte. In textual or graphic representations, the leftmost bit is the MSB. Thus, for example, the most significant bit, b8, of ‘80’ is 1 and the least significant bit, b1, is 0.

All bytes specified as RFU shall be set to '00' and all bits specified as reserved for future use shall be set to 0.

All lengths shall be measured in number of bytes unless otherwise noted.

Data objects in templates are described as being mandatory (M), optional (O) or conditional (C). 'Mandatory' means the data object shall appear in the template. 'Optional' means the data object may appear in the template. In the case of conditional data objects, the conditions under which they are required are provided in a footnote to the table.

In other tables the M/O column identifies properties of the PIV Card Application that shall be present (M) or may be present (O).

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this standard are to be interpreted as described in IETF RFC 2119, Key Words for Use in RFCs to Indicate Requirement Levels [5].

Appendix B—References

[1] Federal Information Processing Standard 201-1, Change Notice 1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006. (See http://csrc.nist.gov)

[2] Government Smart Card Interoperability Specification, Version 2.1, NIST Interagency Report 6887 – 2003 Edition, July 16, 2003.

[3] ISO/IEC 7816 (Parts 4, 5, 6, 8, and 9), *Information technology — Identification cards — Integrated circuit(s) cards with contacts.*

[4] PACS v2.2, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004. http://www.smart.gov/information/TIG_SCEPACS_v2.2.pdf

[5] IETF RFC 2119, "Key Words for Use in RFCs to Indicate Requirement Levels," March, 1997.

[6] *PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version - 1.1* Date - October 01, 2004. Published by authority of the Secretary General, International Civil Aviation Organization.

[7] *DoD CAC Middleware Requirements Release 3.0*, Version 1.0, Access Card Office, March 21, 2006. http://www.smart.gov/iab/documents/DoDcacMiddlewareRequirements.pdf.

[8] *DoD Implementation Guide for CAC Next Generation (NG)*, Version 2.6, DMDC Card Technologies & Identity Solutions Division (CTIS), November, 2006. http://www.smart.gov/iab/documents/CACngImplementationGuide.pdf.