NIST Special Publication 800-73-3

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

Ramaswamy Chandramouli
David Cooper
James F. Dray
Hildegard Ferraiolo
Scott B. Guthery
William MacGregor
Ketan Mehta

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

February 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Dr. Patrick D. Gallagher, 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 Special Publication 800-73-3, Part 4, 20 pages, (February 2010)

Acknowledgements

The authors (Ramaswamy Chandramouli, David Cooper, James Dray, Hildegard Ferraiolo, William MacGregor of NIST, Ketan Mehta of Booz Allen Hamilton, and Scott Guthery of HID Global) 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. 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 12 (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 800-73-3 (SP 800-73-3) 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 in 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 800-73-3 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 800-73-3 enumerates requirements where the standards include options and branches. The specifications go further by constraining implementers' interpretations 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 800-73-3 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 800-73-3 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 interchangeably by all information processing systems across Federal agencies.

Parts 2, 3, and 4 of SP 800-73-3 describe 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 (Parts 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 part, Special Publication 800-73-3, 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.

Readers should also be aware of and familiar with the Revision History section of SP 800-73-3 Part 1.

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:

+ Section 1: *Introduction,* provides the purpose, scope, audience, and assumptions of the document and outlines its structure.
+ Section 2: *Overview and Migration Considerations,* provides the specification that is common to both the transitional and end-point interfaces. Section 2 also includes guidelines as to strategies for migrating from the transitional interfaces to the end-point interfaces.
+ Section 3: *Transition Card Interfaces,* provides links to transitional interface specifications 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. This section is informative.

2. Overview and Migration Considerations

2.1 Migration Considerations

SP 800-73-3 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 800-73-3. Part 4 interface specifications are informative PIV profiles 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 800-73-3, or to implement the End-Point specification 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 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 without prior selection of the file containing the content of the data object.

+ 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 namespace management, the data object identifiers of GSC-IS and transitional systems in the range '0000' through '9FFF'

[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.

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	Container ID	Access Rule for Read	Contact / Contactless[3]	M/O
Card Capability Container	0xDB00	Always	Contact	M
Cardholder Unique Identifier	0x3000	Always	Contact and Contactless	M
X.509 Certificate for PIV Authentication	0x0101	Always	Contact	M
Cardholder Fingerprints	0x6010	PIN	Contact	M
Security Object	0x9000	Always	Contact	M
Cardholder Facial Image	0x6030	PIN	Contact	O
Printed Information	0x3001	PIN	Contact	O
X.509 Certificate for Digital Signature	0x0100	Always	Contact	O
X.509 Certificate for Key Management	0x0102	Always	Contact	O
X.509 Certificate for Card Authentication	0x0500	Always	Contact and Contactless	O
Discovery Object	0x6050	Always	Contact and Contactless	O
Key History Object	0x6060	Always	Contact	O
Retired X.509 Certificate for Key Management 1	0x1001	Always	Contact	O
Retired X.509 Certificate for Key Management 2	0x1002	Always	Contact	O
Retired X.509 Certificate for Key Management 3	0x1003	Always	Contact	O
Retired X.509 Certificate for Key Management 4	0x1004	Always	Contact	O
Retired X.509 Certificate for Key Management 5	0x1005	Always	Contact	O
Retired X.509 Certificate for Key Management 6	0x1006	Always	Contact	O

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

Container Name	Container ID	Access Rule for Read	Contact / Contactless[3]	M/O
Retired X.509 Certificate for Key Management 7	0x1007	Always	Contact	O
Retired X.509 Certificate for Key Management 8	0x1008	Always	Contact	O
Retired X.509 Certificate for Key Management 9	0x1009	Always	Contact	O
Retired X.509 Certificate for Key Management 10	0x100A	Always	Contact	O
Retired X.509 Certificate for Key Management 11	0x100B	Always	Contact	O
Retired X.509 Certificate for Key Management 12	0x100C	Always	Contact	O
Retired X.509 Certificate for Key Management 13	0x100D	Always	Contact	O
Retired X.509 Certificate for Key Management 14	0x100E	Always	Contact	O
Retired X.509 Certificate for Key Management 15	0x100F	Always	Contact	O
Retired X.509 Certificate for Key Management 16	0x1010	Always	Contact	O
Retired X.509 Certificate for Key Management 17	0x1011	Always	Contact	O
Retired X.509 Certificate for Key Management 18	0x1012	Always	Contact	O
Retired X.509 Certificate for Key Management 19	0x1013	Always	Contact	O
Retired X.509 Certificate for Key Management 20	0x1014	Always	Contact	O
Cardholder Iris Images	0x1015	PIN	Contact	O

Part 1, Appendix A provides a detailed spreadsheet for the data model. ContainerIDs and Tags within the containers for each data object are defined by this data model and in accordance with SP 800-73-3 naming conventions.

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

1. Card Capability Container
2. Card Holder Unique Identifier
3. X.509 Certificate for PIV Authentication
4. Cardholder Fingerprints
5. Security Object

The twenty-eight optional data objects for interoperable use are as follows:

1. Cardholder Facial Image
2. Printed Information
3. X.509 Certificate for Digital Signature
4. X.509 Certificate for Key Management
5. X.509 Certificate for Card Authentication
6. Discovery Object
7. Key History Object
8. 20 retired X.509 Certificates for Key Management
9. Cardholder Iris Images

2.3 Mandatory Data Elements

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

2.3.1 Card Capability Container

The Card Capability Container (CCC) is a mandatory data object whose purpose is to facilitate compatibility of GSC-IS applications with End-Point PIV Cards.

The CCC supports minimum capability for retrieval of the data model and optionally the application information as specified in Government Smart Card Interoperability Specification (GSC-IS) [2]. 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 namespace and structure as defined in this document.

For End-Point PIV Card Applications, the PIV data objects exist in a namespace tightly managed by NIST and a CCC discovery mechanism is not needed by End-Point applications. Therefore, all data elements of the CCC, except for the data model number, may optionally have a length value set to zero bytes (i.e., no value field will be supplied). The content of the CCC data elements, other than the data model number, are out of scope for this specification.

2.3.2 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 the 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 in accordance with TIG SCEPACS [4]. A subset of the FASC-N, the FASC-N Identifier, shall be the unique identifier as described in [4, 6.6]: "The combination of an Agency Code, System Code, and Credential Number is a fully qualified number that is uniquely assigned to a single individual". The Agency Code is assigned to each Department or Agency by Special Publication 800-87 (SP 800-87), *Codes for Identification of Federal and Federally-Assisted Organizations* [5]. The subordinate System Code and Credential Number value assignment is subject to Department or Agency policy, provided that the FASC-N identifier (i.e., the concatenated Agency Code, System Code, and Credential Number) is unique for each card. The same FASC-N value shall be used in all the PIV data objects that include the FASC-N. To eliminate unnecessary use of the SSN[4], the FASC-N's Person Identifier (PI) field should not encode the SSN. TIG SCEPACS also specifies PACS interoperability requirements in Section 2.1, 10th paragraph of [4, 2.1]: "For full interoperability of a PACS it must at a minimum be able to distinguish fourteen digits (i.e., a combination of an Agency Code, System Code, and Credential Number) when matching FASC-N based credentials to enrolled card holders."

[4] See the attachment to OMB M-07-16, Section 2: "Reduce the Use of Social Security Numbers".

+ The Global Unique Identification number (GUID) field must be present, and may include either a UUID (see Section 3.3), an issuer assigned IPv6 address[5], or be coded as all zeros (0x00).

+ The DUNS and Organizational Code fields are optional.

+ 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 shall be placed in the signature field of the CHUID.

2.3.3 X.509 Certificate for PIV Authentication

The X.509 Certificate for PIV Authentication and its associated private key, as defined in FIPS 201, is used to authenticate the card and the cardholder. The read access control rule for the X.509 Certificate for PIV Authentication is "Always," meaning the certificate can be read without access control restrictions. The Public Key Infrastructure (PKI) cryptographic function (see Table 3, Part 1) is protected with a "PIN" access rule. In other words, private key operations using the PIV Authentication Key require the Personal Identification Number (PIN) to be submitted, but a successful PIN submission enables multiple private key operations without additional cardholder consent.

2.3.4 Cardholder Fingerprints

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

2.3.5 Security Object

The Security Object is in accordance with Appendix C of PKI for Machine Readable Travel Documents (MRTD) Offering ICC Read-Only Access Version 1.1 [6]. Tag 0xBA is used to map the ContainerIDs in the PIV data model to the 16 Data Groups specified in the 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 refer to the correct hash values in the Security Object (0xBB).

The 0xBB Security Object is formatted according to the MRTD [6, Appendix C]. The LDS Security Object itself must be in ASN.1 DER format, formatted as specified in [6, Appendix C.2]. This

[5] The use of IPv6 addresses in the GUID field is deprecated. It will be removed in a future revision of SP 800-73.

structure is then inserted into the encapContentInfo field of the Cryptographic Message Syntax (CMS) object specified in [6, 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. At a minimum, unsigned data objects, such as the Printed Information data object, shall be included in the Security Object if present. For maximum protection against credential splicing attacks (credential substitution), it is recommended, however, that all PIV data objects, except the PIV X.509 certificates, be included in the Security Object.

2.4 Optional Data Elements

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

2.4.1 Cardholder Facial Image

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

2.4.2 Printed Information

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.

2.4.3 X.509 Certificate for Digital Signature

The X.509 Certificate for Digital Signature and its associated private key, as defined in FIPS 201, support the use of digital signatures for the purpose of document signing. The read access control rule for the X.509 Certificate is "Always", meaning the certificate can be read without access control restrictions. The PKI cryptographic function is protected with a "PIN Always" access rule. In other words, the PIN must be submitted every time immediately before a *Digital Signature Key* operation. This ensures cardholder participation every time the private key is used for digital signature generation.

2.4.4 X.509 Certificate for Key Management

The X.509 Certificate for Key Management and its associated private key, as defined in FIPS 201, support the use of encryption for the purpose of confidentiality. This key pair may be escrowed by the issuer for key recovery purposes. The read access control rule for the X.509 Certificate is "Always", meaning the certificate can be read without access control restrictions. 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 the PIN again. This enables multiple private key operations without additional cardholder consent.

2.4.5 X.509 Certificate for Card Authentication

FIPS 201 specifies the optional Card Authentication Key (CAK) as an asymmetric or symmetric key that is used to support additional physical access applications. For an asymmetric CAK, the read

access control rule of the corresponding X.509 Certificate for Card Authentication is "Always", meaning the certificate can be read without access control restrictions. Private (asymmetric) key operations or secret (symmetric) key operations are defined as "Always". In other words, the private or secret key can be used without access control restrictions. If the CAK is implemented, an asymmetric or symmetric CAK is generated by the PIV Card Issuer in accordance with FIPS 140-2 requirements for key generation. A CAK may be generated on-card or off-card. If a CAK is generated off-card, the result of each key generation will be injected into at most one PIV Card.

2.4.6 Discovery Object

The Discovery Object, if implemented, is the 0x7E interindustry ISO/IEC 7816-6 template that nests interindustry data objects. For the Discovery Object, the 0x7E template nests two BER-TLV structured interindustry data elements: 1) tag 0x4F contains the AID of the PIV Card Application and 2) tag 0x5F2F lists the PIN Usage Policy.

+ Tag 0x4F encodes the PIV Card Application AID as follows:

  {'4F 0B A0 00 00 03 08 00 00 10 00 01 00'}

+ Tag 0x5F2F encodes the PIN Usage Policy as follows:

  First byte: 0x40 indicates that the PIV Card Application PIN alone satisfies the PIV Access Control Rules (ACRs) for command execution[6] and object access.

  0x60 indicates that both the PIV Card Application PIN and Global PIN satisfy the PIV ACRs for command execution and PIV data object access.

  Bits 5 through 1 of the first byte are RFU.

  The second byte of the PIN Usage Policy encodes the cardholder's PIN preference for PIV Cards with both the PIV Card Application PIN and the Global PIN enabled:

  Second byte: 0x10 indicates that the PIV Card Application PIN is the primary PIN used to satisfy the PIV ACRs for command execution and object access.

  0x20 indicates that the Global PIN is the primary PIN used to satisfy the PIV ACRs for command execution and object access.

Note: If the first byte is set to 0x40, then the second byte is RFU and shall be set to 0x00.

PIV Card Applications that satisfy the PIV ACRs for PIV data object access and command execution[7] with both the PIV Card Application PIN and Global PIN shall implement the Discovery Object with the PIN Usage Policy set to 0x60 zz where zz is set to either 0x10 or 0x20.

The encoding of the 0x7E Discovery Object is as follows:

{'7E 12' {{'4F 0B A0 00 00 03 08 00 00 10 00 01 00'} {'5F 2F 02 xx yy'}}}, where xx and yy encode the first and second byte of the PIN Usage Policy as described in this section.

[6] Command execution pertains to the VERIFY APDU and optionally to the CHANGE REFERENCE DATA APDU.
[7] Command execution pertains to the VERIFY APDU and optionally to the CHANGE REFERENCE DATA APDU.

The Security Object enforces integrity of the Discovery Object according to the issuer.

2.4.7 Key History Object

Up to twenty retired Key Management private keys may be stored in the PIV Card Application. The Key History object provides information about the retired Key Management private keys that are present within the PIV Card Application. Retired Key Management private keys are private keys that correspond to X.509 certificates for Key Management that have expired, have been revoked, or have otherwise been superseded. The Key History object shall be present in the PIV Card Application if the PIV Card Application contains any retired Key Management private keys, but may be present even if no such keys are present in the PIV Card Application. For each retired Key Management private key in the PIV Card Application, the corresponding certificate may either be present within the PIV Card Application or may only be available from an on-line repository.

The Key History object includes two mandatory fields, *keysWithOnCardCerts* and *keysWithOffCardCerts*, and one optional field, *offCardCertURL*. The *keysWithOnCardCerts* field indicates the number of retired private keys within the PIV Card Application for which the corresponding certificates are also stored within the PIV Card Application. The *keysWithOffCardCerts* field indicates the number of retired private keys within the PIV Card Application for which the corresponding certificates are not stored within the PIV Card Application. The numeric values in both *keysWithOnCardCerts* and *keysWithOffCardCerts* are represented as unsigned binary integers. The *offCardCertURL* field contains a URL that points to a file containing the certificates corresponding to all of the retired private keys within the PIV Card Application, including those for which the corresponding certificate is also stored within the PIV Card Application. The *offCardCertURL* field shall be present if the *keysWithOffCardCerts* value is greater than zero and shall be absent if the values of both *keysWithOnCardCerts* and *keysWithOffCardCerts* are zero. The *offCardCertURL* field may be present if the *keysWithOffCardCerts* value is zero but the *keysWithOnCardCerts* value is greater than zero.

The file that is pointed to by the *offCardCertURL* field shall contain the DER encoding of the following data structure:

```
OffCardKeyHistoryFile ::= SEQUENCE SIZE (1..20) OF SEQUENCE {
        keyReference        OCTET STRING (SIZE(1))
        cert                Certificate
}
```

where **keyReference** is the key reference for the private key on the card and **cert** is the corresponding X.509 certificate.[8] The *offCardCertURL* field shall have the following format:

"http://" <DNS name> "/" <ASCII-HEX encoded SHA-256 hash [13] of **OffCardKeyHistoryFile**>

The private keys for which the corresponding certificates are stored within the PIV Card Application shall be assigned to the lowest numbered key references reserved for retired Key Management private keys. For example if *keysWithOnCardCerts* is 5, then the corresponding private keys shall be assigned to key references '82', '83', '84', '85', and '86'.

The private keys for which the corresponding certificates are not stored within the PIV Card Application shall be assigned to the highest numbered key references reserved for retired Key

[8] The ASN.1 for **Certificate** may be imported from the ASN.1 module **PKIX1Explicit88** in Appendix A.1 of RFC 5280 [12].

Management private keys. For example, if *keysWithOffCardCerts* is 3, then the corresponding private keys shall be assigned to key references '93', '94', and '95'.

Private keys do not have to be stored within the PIV Card Application in the order of their age. However, if the certificates corresponding to only some of the retired Key Management private keys are available within the PIV Card Application then the certificates that are stored in the PIV Card Application shall be the ones that were most recently issued.

The Key History object is only available over the contact interface. The read access control rule for the Key History object is "Always", meaning that it can be read without access control restrictions.

The Security Object enforces integrity of the Key History object according to the issuer.

2.4.8 Retired X.509 Certificates for Key Management

These objects hold the X.509 certificates for Key Management corresponding to retired Key Management Keys, as described in Section 2.4.7. Retired Key Management private keys and their corresponding certificates are only available over the contact interface. The read access control rule for these certificates is "Always", meaning the certificates can be read without access control restrictions. The PKI cryptographic function for all of the retired Key Management Keys is protected with a "PIN" access rule. In other words, once the PIN is submitted and verified, subsequent *Key Management Key* operations can be performed with any of the retired Key Management Keys without requiring the PIN again. This enables multiple private key operations without additional cardholder consent.

2.4.9 Cardholder Iris Images

The iris data object specifies compact images of the cardholder's irises. The images are suitable for use in iris recognition systems for automated identity verification.

2.5 Inclusion of Universally Unique IDentifiers (UUIDs)

As defined in [9], the presence of a Universally Unique IDentifier (UUID) conformant to the specification [10] is required in each identification card issued by Non-Federal Issuers, referred to as "PIV Interoperable" (PIV-I) or "PIV Compatible" (PIV-C) cards. The intent of [9] is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Department or Agency. Because the goal is interoperability of PIV-I and PIV-C cards with the Federal PIV System, the technical requirements for the inclusion of the UUID are specified in this document. To include a UUID identifier on a PIV-I, PIV-C, or PIV Card, a credential issuer shall meet the following specifications for all relevant data objects present on an issued identification card.

1. If the card is a PIV-I or PIV-C card, the FASC-N in the CHUID shall have Agency Code equal to 9999, System Code equal to 9999, and Credential Number equal to 999999, indicating that a UUID is the primary credential identifier. In this case, the FASC-N shall be omitted from certificates and CMS-signed data objects. If the card is a PIV Card, the FASC-N in the CHUID shall be populated as described in Section 2.3.2, and the FASC-N shall be included in authentication certificates and CMS-signed data objects as required by FIPS 201.

2. The value of the GUID data element of the CHUID data object shall be a 16-byte binary representation of a valid UUID [10]. The UUID should be version 1, 4, or 5, as specified in [10], Section 4.1.3.

3. The same 16-byte binary representation of the UUID value shall be present as the value of an entryUUID attribute, as defined in [11], in any CMS-signed data object that is required to contain a pivFASC-N attribute on a PIV Card, i.e., in the fingerprint template and facial image data objects, if present.

4. The string representation of the same UUID value shall be present in the PIV Authentication Certificate and the Card Authentication Certificate, if present, in the subjectAltName extension encoded as a URI, as specified by [10], Section 3.

The option specified in this section supports the use of UUIDs by Non-Federal Issuers. It also allows, but does not require, the use of UUIDs as optional data elements on PIV Cards. PIV Cards must meet all requirements in FIPS 201 whether or not the UUID identifier option is used; in particular, the FASC-N identifier must be present in all PIV data objects as specified by FIPS 201 and its normative references. PIV Cards that include UUIDs must include the UUIDs in all data objects described in (2) through (4).

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

ACR	Access Control Rule
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
BSI	Basic Services Interface
CAK	Card Authentication Key
CBEFF	Common Biometric Exchange Formats Framework
CCC	Card Capability Container
CHUID	Card Holder Unique Identifier
CMS	Cryptographic Message Syntax
DG	Data Group
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
HSPD	Homeland Security Presidential Directive
ICC	Integrated Circuit Card
IEC	International Electrotechnical Commission
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
LSB	Least Significant Bit
MRTD	Machine Readable Travel Document
MSB	Most Significant Bit
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
PACS	Physical Access Control System
PI	Person Identifier, a field in the FASC-N
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIV-C	PIV Compatible
PIV-I	PIV Interoperable
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
RFU	Reserved for Future Use
RID	Registered application provider IDentifier
RSA	Rivest, Shamir, Adleman
SCEPACS	Smart Card Enabled Physical Access Control System
SHA	Secure Hash Algorithm
SP	Special Publication

TIG	Technical Implementation Guidance
TLV	Tag-Length-Value
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique IDentifier
TIG	Technical Implementation Guidance
VM	Virtual Machine

A.3 Notation

The sixteen hexadecimal digits shall be denoted using the alphanumeric characters 0, 1, 2, …, 9, 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).

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.
(See http://fips201ep.cio.gov/documents/TIG_SCEPACS_v2.2.pdf)

[5] NIST Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*, April 2008. (See http://csrc.nist.gov)

[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. (See 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.
(See http://www.smart.gov/iab/documents/CACngImplementationGuide.pdf)

[9] *Personal Identity Verification Interoperability For Non-Federal Issuers*, May 2009.
(See http://www.idmanagement.gov)

[10] IETF RFC 4122, "A Universally Unique IDentifier (UUID) URN Namespace," July 2005.

[11] IETF RFC 4530, "Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute," June 2006.

[12] IETF RFC 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," May 2008.

[13] Federal Information Processing Standard 180-3, *Secure Hash Standard (SHS)*, October 2008.
(See http://csrc.nist.gov)