NIST Special Publication 800-73-2
2nd DRAFT

Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model, and Representation

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

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

INFORMATION SECURITY

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 Special Publication 800-73-2, Part 1, 40 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

List of Figures

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) contains technical specifications to interface with the smart card (PIV Card[1]) to retrieve and use the identity credentials.

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 this document. 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. SP 800-73 defines the PIV data elements identifiers, structure and format. SP 800-73 also describes the client application programming interface and card command interface for use of the PIV card.

This first Part, Special Publication 800-73 (SP 800-73) Part 1 – *End-Point PIV Card Application Namespace, Data Model and Representation*, specifies the End-Point PIV Card Application Namespace, the PIV Data Model and its logical representation on the PIV card and is a companion document to FIPS 201.

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 1 is organized as follows:

+ Section 1, *Introduction*, provides the purpose, scope, audience, and assumptions of the document and outlines its structure.
+ Section 2, *PIV Card Application Namespace,* defines the three NIST managed namespaces used by the PIV card application.
+ Section 3, End-Point *PIV Data Model Elements*, describes the PIV Data Model Elements in detail.
+ Section 4, *End-Point PIV Data Objects Representation*, describes the format and coding of the PIV data structures used by the PIV client-application programming interface and the PIV Card Application.
+ Section 5, *End-Point Data Types and Their Representation,* provides the details of the data types found on the PIV client-application programming interface and the PIV card Application card command interface.

1.5.1 Appendices

The appendices contain material needing special formatting together with illustrative material to aid in understanding information in the body of the document.

2. PIV Card Application Namespaces

2.1 Namespaces of the PIV Card Application

Names used on the PIV interfaces are drawn from three namespaces managed by NIST:

+ Proprietary Identifier eXtension (PIXes) of the NIST registered application provider Identifier (RID)
+ ASN.1 object identifiers (OIDs) in the personal verification subset of the OIDs managed by NIST
+ Basic Encoding Rules – Tag Length Value (BER-TLV) tags of the NIST PIV coexistent tag allocation scheme

All unspecified names in these managed namespaces are reserved for future use.

All interindustry tags defined in ISO/IEC 7816, Information Technology – Identification Cards – Integrated Circuit(s) Card with Contacts [2], and used in the NIST coexistent tag allocation scheme without redefinition have the same meaning in the NIST PIV coexistent tag allocation scheme as they have in [2].

All unspecified values in the following identifier and value namespaces are reserved for future use:

+ algorithm identifiers
+ key reference values
+ cryptographic mechanism identifiers

2.2 PIV Card Application AID

The Application Identifier (AID) of the Personal Identity Verification card application (PIV Card Application) shall be:

'A0 00 00 03 08 00 00 10 00 01 00’

The AID of the PIV Card Application consists of the NIST RID (‘A0 00 00 03 08’) followed by the application portion of the NIST PIX indicating the PIV Card Application (’00 00 10 00’) and then the version portion of the NIST PIX (’01 00’) for the version of the PIV Card Application. All other PIX sequences on the NIST RID including the trailing five bytes PIV Card Application AID are reserved for future use.

The PIV Card Application can be selected as the current application by providing the full AID as listed above or by providing the right-truncated version; that is, without the two-byte version as follows:

'A0 00 00 03 08 00 00 10 00’

3. End-Point PIV Data Model Elements

This section contains the description of the data elements for personal identity verification, the PIV data model.

A PIV Card Application shall contain five mandatory interoperable data objects and may contain six 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. Card Holder Fingerprints
5. Security Object

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

1. Card Holder 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. PIV Discovery Object

3.1 Mandatory Data Elements

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

3.1.1 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.

3.1.2 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. The Public Key Infrastructure (PKI) cryptographic function is protected with a "Always" access rule. In other words, private key operations with the PIV Authentication Key requires the Personal Identification Number (PIN), but enables multiple compute operations without additional cardholder consent.

3.1.3 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 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[2] 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.

3.1.4 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.

3.1.5 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.

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

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[3] if present.

3.2 Optional Data Elements

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

3.2.1 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.

3.2.2 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.

3.2.3 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.

3.2.4 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

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

requiring PIN again. This requires cardholder activation, but enables multiple compute operations without additional cardholder consent.

3.2.5 X.509 Certificate for Card Authentication

This key and certificate (if the key is an asymmetric key) support 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. With extremely high probability, each PIV Card shall contain a unique Card Authentication Key.

3.2.6 PIV Discovery Object

The PIV Discovery Object, if implemented, is the '7E' interindustry ISO/IEC 7816-6 template that nests interindustry data objects. For the PIV Discovery Object , the'7E' template nests two BER-TLV structured interindustry data elements: 1) tag '4F' contains the AID of the PIV card application and 2) tag '5F2F' lists the PIN Usage Policy.

+ Tag '4F' 'encodes the PIV Card Application AID as follows:
  {'4F 0B A0 00 00 03 08 00 00 10 00 01 00'}

+ Tag '5F2F' is encoded as follows:

  First byte: '40' indicates that the PIV PIN alone satisfies the PIV ACRs for command execution[4] and object access.
  '60' indicates that both PIV 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.
  Second byte: The second byte is RFU and shall be set to '00'.

Thus, the encoding of the'7E' PIV Discovery Object is as follows:

{'7E 0C' {{'4F 0B A0 00 00 03 08 00 00 10 00 01 00'} {'5F 2F 02 x0 00'}}

PIV card application that satisfy the PIV ACRs for PIV data object access and command execution with both PIV PIN and Global PIN shall implement the PIV Discovery Object with the PIN Usage Policy set to '60'.

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

3.3 Data Object Containers and associated Access Rules and Interface Modes

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.

[4] Command execution pertains to the following commands: 1) VERIFY, 2) CHANGE REFERENCE DATA, 3)RESET RETRY COUNTER

Table 1. Data Model Containers

Container Name	ContainerID	Access Rule for Read	Contact / Contactless[5]	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
PIV Discovery Object	0x6050	Always	Contact	Optional

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 accord with SP 800-73 naming conventions.

[5] 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.

4. End Point PIV Data Objects Representation

4.1 Data Objects Definition

A *data object* is an item of information seen on the card command interface for which are specified a name, a description of logical content, a format and a coding. Each data object has a globally unique name called its *object identifier* as defined in ISO/IEC 8824-2:2002, Information technology – Abstract Syntax Notation One (ASN.1): Information object specification. [6]

A data object whose 1:2002, Information technology data content is encoded as a BER-TLV data structure as in ISO/IEC 8825-– ASN.1 encoding rules, [7] is called *BER-TLV data object.*

4.1.1 Data Object Content

The *content* of a data object is the sequence of bytes that are said to be *contained in* or to be the *value of* the data object. The number of bytes in this byte sequence is referred to as the *length* of the data content and also as the *size* of the data object. The first byte in the sequence is regarded as being at *byte position* or *offset* zero in the content of the data object.

The data content of a BER-TLV data object may consist of other BER-TLV data objects. In this case the tag of the data object indicates that data object is a *constructed data object*. A BER-TLV data object that is not a constructed data object is called a *primitive data object*.

The PIV End-Point Data objects are BER-TLV objects encoded as per ISO/IEC 8825-2, except that tag values (T-values) of the PIV data object's inner tag assignments do not conform to BER-TLV requirements. This is due to the need to accommodate legacy tags inherited from the GSC-IS specification.

4.2 OIDs and Tags of PIV Card Application Data Objects

Table 2 lists the ASN.1 object identifiers and BER-TLV tags of the ten PIV Card Application data objects for interoperable use. For the purpose of constructing PIV Card Application data object names in the CardApplicationURL in CCC of the PIV Card Application, the NIST RID (‘A0 00 00 03 08’) shall be used and the card application type shall be set to ‘00’.

4.3 Object Identifiers

Each of the data objects in the PIV Card Application has been provided with an ASN.1 OID from the NIST personal verification arc and a three-byte BER-TLV tag. These object identifier assignments are given in Table 2.

A data object shall be identified on the PIV client-application programming interface using its OID. An object identifier on the PIV client-application programming interface shall be a dot delimited string of the integer components of the OID. For example, the representation of the OID of the CHUID on the PIV client-application programming interface is “2.16.840.1.101.3.7.2.48.0”.

A data object shall be identified on the PIV Card Application card command interface using its BER-TLV tag. For example, the CHUID is identified on the card command interface to the PIV Card Application by the three-byte identifier ‘5FC102’.

Table 1 lists the access control rules of the ten PIV Card Application data objects for interoperable use. See table 6-3 in Special Publication 800-78 (SP 800-78) *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* [8], for the key references and permitted algorithms associated with these authenticatable entities.

Table 2. Object Identifiers of the PIV Data Objects for Interoperable Use

Data Object for Interoperable Use	ASN.1 OID	BER-TLV Tag	M/O
Card Capability Container	2.16.840.1.101.3.7.1.219.0	'5FC107'	M
Card Holder Unique Identifier	2.16.840.1.101.3.7.2.48.0	'5FC102'	M
X.509 Certificate for PIV Authentication	2.16.840.1.101.3.7.2.1.1	'5FC105'	M
Card Holder Fingerprints	2.16.840.1.101.3.7.2.96.16	'5FC103'	M
Printed Information	2.16.840.1.101.3.7.2.48.1	'5FC109'	O
Card Holder Facial Image	2.16.840.1.101.3.7.2.96.48	'5FC108'	O
X.509 Certificate for Digital Signature	2.16.840.1.101.3.7.2.1.0	'5FC10A'	O
X.509 Certificate for Key Management	2.16.840.1.101.3.7.2.1.2	'5FC10B'	O
X.509 Certificate for Card Authentication	2.16.840.1.101.3.7.2.5.0	'5FC101'	O
Security Object	2.16.840.1.101.3.7.2.144.0	'5FC106'	M
PIV Discovery Object	2.16.840.1.101.3.7.2.5.1	'7E'	O

5. End-Point Data Types and Their Representation

This section provides a description of the data type used in the PIV Client-application Programming Interface (SP 800-73, Part 3) and PIV Card Command Interface (SP 800-73, Part 2). Unless otherwise indicated, the representation shall be the same on both interfaces.

The data types are defined in Part 1, rather than in Parts 2 and 3 in order to achieve smart card platform independence from Part 1. Thus, non-government smartcard programs can readily adopt the interface specifications in Parts 2 and 3 while customizing Part 1 to their own data model, data types, and namespaces.

5.1 Key References

A PIV key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. SP 800-78, Table 6-1 defines the key reference values that shall be used on the PIV interfaces. The Key reference values are used in a cryptographic protocol such as an authentication or a signing protocol. Key references are only assigned to private and secret (symmetric) keys. All other PIV Card Application key reference values are reserved for future use.

Table 3. PIV Card Application Authentication and Key References

Key Reference Value	PIV Key Type	Authenticatable Entity / Administrator	Security Condition for Use	Retry Reset Value	Number of Unblocks
'00'	Global PIN	Card Holder	Always	Platform Specific	Platform Specific
'80'	Application PIN	Card Holder	Always	Issuer Specific	Issuer Specific
'81'	PIN Unblock Key	PIV Card Application Administrator	Always	Issuer Specific	Issuer Specific
See Table 6-1 in SP 800-78	*PIV Authentication Key*	PIV Card Application Administrator	PIN	N/A	N/A
See Table 6-1 in SP 800-78	*Card Management Key*[6]	PIV Card Application Administrator	Always	N/A	N/A
See Table 6-1 in SP 800-78	*Digital Signature Key*	PIV Card Application Administrator	PIN Always	N/A	N/A
See Table 6-1 in SP 800-78	*Key Management Key*	PIV Card Application Administrator	PIN	N/A	N/A
See Table 6-1 in SP 800-78	*Card Authentication Key*	PIV Card Application Administrator	Always	N/A	N/A

[6] Note: The Card Management key is the PIV Card Application Administration Key used for managing PIV application.

When represented as a byte, the key reference occupies b8 and b5-b1 while b7 and b6 shall be set to 0. If b8 is 0 then the key reference names global reference data. If b8 is 1 then the key reference names application-specific reference data.

The Access Control Rules for PIV data object access shall reference the PIV card application PIN and may optionally reference the card holder global PIN. If the Global PIN is used by the PIV card application, the Global PIN format shall follow the PIV PIN format defined in section 2.4.3 of Part 2.

PIV card application with the PIV discovery object, and the first byte of the PIN Usage Policy value set to '60' as per section 3.2.6, shall reference the PIV card application PIN as well as the card holder global PIN in the Access Control Rules for PIV data object access Additionally, the PIV card application card commands can change status of the global PIN, change its reference data, and reset its retry counter while the PIV Card Application is the currently selected application.

Note: The rest of the document uses "PIN" to mean either the PIV Application PIN or the Global PIN.

5.2 PIV Algorithm Identifier

A PIV algorithm identifier shall be a one-byte identifier of a cryptographic algorithm. The identifier specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of operation (i.e., CBC or ECB). SP 800-78, Table 6-2 lists the PIV algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV interfaces.

5.3 Cryptographic Mechanism Identifiers

Cryptographic Mechanism Identifiers are defined in Table 4. These identifiers serve as data field inputs to the GENERATE ASYMMETRIC KEY PAIR card command and pivGenerateKeyPair client API, which initiates the generation and storing of the asymmetric key pair.

Table 4. Cryptographic Mechanism Identifiers

Cryptographic Mechanism Identifier	Description	Parameter
'00'-'05'	RFU	
See Table 6-2 in SP 800-78	RSA 1024	Optional public exponent encoded big-endian
See Table 6-2 in SP 800-78'	RSA 2048	Optional public exponent encoded big-endian
'08'-'10'	RFU	
See Table 6-2 in SP 800-78	ECC: Curve P-256	None
'12'-'13'	RFU	
See Table 6-2 in SP 800-78	ECC: Curve P-384	None

All other cryptographic mechanism identifier values are reserved for future use.

5.4 Status Words

A status word shall be a 2-byte value returned by an entry point on the client-application programming interface or a card command at the card edge. The first byte of a status word is referred to as SW1 and the second byte of a status word is referred to as SW2.

Recognized values of all SW1-SW2 pairs used as return values on both the client-application programming and card command interfaces and their interpretation are given in Table 5. The description of individual client-application programming interface entry points or card commands provide additional information for interpreting the status words they return.

Table 5. Status Words

SW1	SW2	Meaning
'61'	'xx'	Successful execution where SW2 encodes the number of response data bytes still available
'63'	'CX'	Verification failed, X indicates the number of further allowed retries or resets
‘69’	‘82’	Security condition not satisfied
‘69’	‘83’	Authentication method blocked
‘6A’	‘80’	Incorrect parameter in command data field
‘6A’	‘81’	Function not supported
'6A'	'84'	Not enough memory
‘6A’	‘86’	Incorrect parameter in P1 or P2
‘6A’	‘88’	Referenced data or reference data not found
'90'	'00'	Successful execution

Appendix A—PIV Data Model

The PIV data model number is 0x10, and the data model version number is 0x01.

The SP800-73 End-Point specification does not provide mechanisms to read partial contents of a PIV data object. Individual access to the TLV elements within a container is not supported. End-Point compliant cards shall return all TLV elements of a container in the order listed for that container in this data model.

Both single-chip/dual-interface and dual-chip implementations shall be feasible. In the single-chip/dual-interface configuration, the PIV Card Application shall be provided the information regarding which interface is in use. In the dual-chip configuration, a separate PIV Card Application shall be loaded on each chip.

Table 6. PIV Data Containers

Container Description	Container ID	BER-TLV Tag	Container Minimum Capacity (Bytes)*	Access Rule for Read	Contact / Contactless	M/O
Card Capabilities Container	0xDB00	'5FC107'	297	Always	Contact	M
Card Holder Unique Identifier	0x3000	'5FC102'	3414	Always	Contact and Contactless	M
X.509 Certificate for PIV Authentication	0x0101	'5FC105'	2005	Always	Contact	M
Card Holder Fingerprints	0x6010	'5FC103'	4006	PIN	Contact	M
Printed Information	0x3001	'5FC109'	164	PIN	Contact	O
Card Holder Facial Image	0x6030	'5FC108'	12710	PIN	Contact	O
X.509 Certificate for Digital Signature	0x0100	'5FC10A'	2005	Always	Contact	O
X.509 Certificate for Key Management	0x0102	'5FC10B'	2005	Always	Contact	O
X.509 Certificate for Card Authentication	0x0500	'5FC101'	2005	Always	Contact and Contactless	O
Security Object	0x9000	'5FC106'	1031	Always	Contact	M
PIV Discovery Object	0x6050	'7E'	20	Always	Contact	O

* The values in this column denote the guaranteed minimum capacities, in bytes, of the on-card storage containers. Cards may be produced and determined conformant with larger containers.

Note that all data elements of the following data objects are mandatory unless specified as optional.

Table 7. Card Capabilities Container

Card Capabilities Container	0xDB00		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Card Identifier	0xF0	Fixed	21
Capability Container version number	0xF1	Fixed	1
Capability Grammar version number	0xF2	Fixed	1
Applications CardURL	0xF3	Variable	128
PKCS#15	0xF4	Fixed	1
Registered Data Model number	0xF5	Fixed	1
Access Control Rule Table[7]	0xF6	Fixed	17
CARD APDUs	0xF7	Fixed	0
Redirection Tag	0xFA	Fixed	0
Capability Tuples (CTs)	0xFB	Fixed	0
Status Tuples (STs)	0xFC	Fixed	0
Next CCC	0xFD	Fixed	0
Extended Application CardURL (optional)	0xE3	Fixed	48
Security Object Buffer (optional)	0xB4	Fixed	48
Error Detection Code	0xFE	LRC	0

Table 8. Card Holder Unique Identifier

Card Holder Unique Identifier	0x3000		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Buffer Length (Optional)	0xEE	Fixed	2
FASC-N	0x30	Fixed Text	25
Organization Identifier (Optional)	0x32	Fixed	4
DUNS (Optional)	0x33	Fixed	9
GUID	0x34	Fixed Numeric	16
Expiration Date	0x35	Date (YYYYMMDD)	8
Authentication Key Map (Optional)	0x3D	Variable	512
Issuer Asymmetric Signature	0x3E	Variable	2816
Error Detection Code	0xFE	LRC	0

* The values in the “Max. Bytes” columns denote the lengths of the value (V) fields of BER-TLV elements.

Table 9. X.509 Certificate for PIV Authentication

X.509 Certificate for PIV Authentication	0x0101		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Certificate	0x70	Variable	1856**
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 10. Card Holder Fingerprints

Card Holder Fingerprints	0x6010		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Fingerprint I & II	0xBC	Variable	4000
Error Detection Code	0xFE	LRC	0

Table 11. Printed Information

Printed Information	0x3001		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Name	0x01	Fixed Text	32
Employee Affiliation (Line 1)	0x02	Fixed Text	20
Employee Affiliation (Line 2)	0x03	Fixed Text	20
Expiration date	0x04	Date (YYYYMMMDD)	9
Agency Card Serial Number	0x05	Fixed Text	10
Issuer Identification	0x06	Fixed Text	15
Organization Affiliation (Line 1) (Optional)	0x07	Fixed Text	20
Organization Affiliation (Line 2) (Optional)	0x08	Fixed Text	20
Error Detection Code	0xFE	LRC	0

Note: The Organization Affiliation fields (tags 0x07 and 0x08) are new optional data elements in the Printed Information data object. Employee Affiliation Line 2 (tag 0x03) is deprecated and will be eliminated in a future revision, as it does not have a corresponding text field on the face of the card. In order to successfully match the printed information for verification on Zone 8 (Employee Affiliation) and Zone 10 (Organization Affiliation) on the face of the card with the printed information represented stored electronically on card, agencies should use tags 0x02, 0x07 and 0x08.

* The values in the "Max. Bytes" columns denote the lengths of the value (V) fields of BER-TLV elements.
** Recommended length. Certificate size can exceed indicated length value.

Table 12. Card Holder Facial Image

Card Holder Facial Image		0x6030	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Image for Visual Verification	0xBC	Variable	12704
Error Detection Code	0xFE	LRC	0

Table 13. X.509 Certificate for Digital Signature

X.509 Certificate for Digital Signature		0x0100	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Certificate	0x70	Variable	1856**
CertiInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 14. X.509 Certificate for Key Management

X.509 Certificate for Key Management		0x0102	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Certificate	0x70	Variable	1856**
CertiInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 15. X.509 Certificate for Card Authentication

X.509 Certificate for Card Authentication		0x0500	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Certificate	0x70	Variable	1856**
CertiInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 16. Security Object

Security Object		0x9000	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Mapping of DG to ContainerID	0xBA	Variable	100
Security Object	0xBB	Variable	900
Error Detection Code	0xFE	LRC	0

* The values in the "Max. Bytes" columns denote the lengths of the value (V) fields of BER-TLV elements.
** Recommended length. Certificate size can exceed indicated length value.

The CertInfo byte in certificates identified above shall be encoded as follows:

```
CertInfo::= BIT STRING {
                    CompressionTypeMsb(0),  // 0 = no compression and 1 = gzip[8] compression.
                    CompressionTypeLsb(1),  // shall be set to '0' for PIV Applications
                    IsX509(2),              // shall be set to '0' for PIV Applications
                    RFU3(3),
                    RFU4(4),
                    RFU5(5),
                    RFU6(6),
                    RFU7(7)
                    }
```

Table 17. PIV Discovery Object

PIV Discovery Object (Tag '7E')		0x6050	
PIV AID BER TLV	0x4F	Fixed	12
PIV PIN Usage Policy	0x5F 2F	Fixed	3

[8]Gzip formats are specified in RFC 1951 and RFC 1952

Appendix B—PIV Authentication Use Cases

To provide guidelines on the usage and behavior supported by the PIV Card, PIV authentication use cases and application scenarios are described in this section. FIPS 201 describes PIV authentication as the "process of establishing confidence in the identity of the cardholder presenting a PIV Card." The fundamental goal of using the PIV Card is to authenticate the identity of the cardholder to a system or person that is controlling access to a protected resource or facility. This end goal may be reached by various combinations of one or more of the validation steps described below:

Card Validation (CardV) — This is the process of verifying that a PIV Card is authentic (i.e., not a counterfeit card). Card validation mechanisms include:

+ Visual inspection of the tamper-proofing and tamper-resistant features of the PIV Card as per Section 4.1.2 of FIPS 201,
+ Use of cryptographic challenge-response schemes with symmetric keys,
+ Use of asymmetric authentication schemes to validate private keys embedded within the PIV Card.

Credential Validation (CredV) — This is the process of verifying the various types of credentials (such as visual credentials, CHUID, biometrics, PIV keys and certificates) held by the PIV Card. Credential validation mechanisms include:

+ Visual inspection of PIV Card visual elements (such as the photo, the printed name, and rank, if present),
+ Verification of certificates on the PIV Card,
+ Verification of signatures on the PIV biometrics and the CHUID,
+ Checking the expiration date,
+ Checking the revocation status of the credentials on the PIV Card.

Cardholder Validation (HolderV) — This is the process of establishing that the PIV Card is in the possession of the individual who is the legitimate owner of the card. Classically, identity authentication is achieved using one or more of these factors: a) something you have, b) something you know, and c) something you are. The assurance of the authentication process increases with the number of factors used. In the case of the PIV Card, these three factors translate as follows: a) something you have – possession of a PIV Card, b) something you know – knowledge of the PIN, and c) something you are – the visual characteristics of the cardholder, and the live fingerprint samples provided by the cardholder. Thus, mechanisms for PIV cardholder validation include:

+ Presentation of a PIV Card by the cardholder,
+ Matching the visual characteristics of the cardholder with the photo on the PIV Card,
+ Matching the PIN provided with the PIN on the PIV Card,

+ Matching the live fingerprint samples provided by the cardholder, with the biometric information embedded within the PIV Card.

B.1 Use Case Diagrams

This section describes the activities and interactions involved in interoperable usage and authentication of the PIV Card. The use cases represent how a relying party will authenticate the cardholder (regardless of which agency issued the card) in order to provide access to its systems or facilities. These activities and interactions are represented in functional use case diagrams. These diagrams are not intended to provide syntactical commands or API function names.

Each of the PIV authentication mechanisms described in this section can be broken into a sequence of one or more validation steps where Card, Credential, and Cardholder validation is performed. In the use case illustrations, the validation steps are marked as CardV, CredV and HolderV to signify Card, Credential, and Cardholder validation respectively.

Depending upon the assurance provided by the actual sequence of validation steps in a given PIV authentication mechanism, relying parties can make appropriate decisions for granting access to protected resources based on a risk analysis.

B.1.1 Authentication using PIV Visual Credentials

This is the use case where a human guard authenticates the cardholder using the visual credentials held by the PIV Card, and is illustrated in Figure B-1.

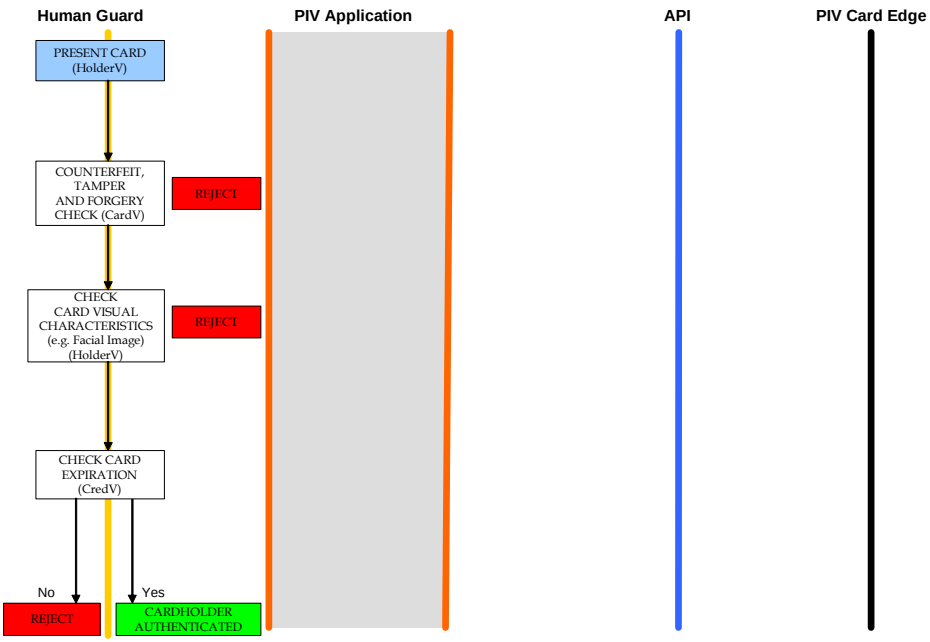

Figure B-1. Authentication using PIV Visual Credentials

B.1.2 Authentication using PIV CHUID

The PIV CHUID may be used for authentication in several variations. The use of the PIV Card to implement the CHUID use case is illustrated in Figure B-2. The minimum set of data that must be transmitted from the PIV Application on the Local System to the host is application dependent and therefore not defined in this Specification.

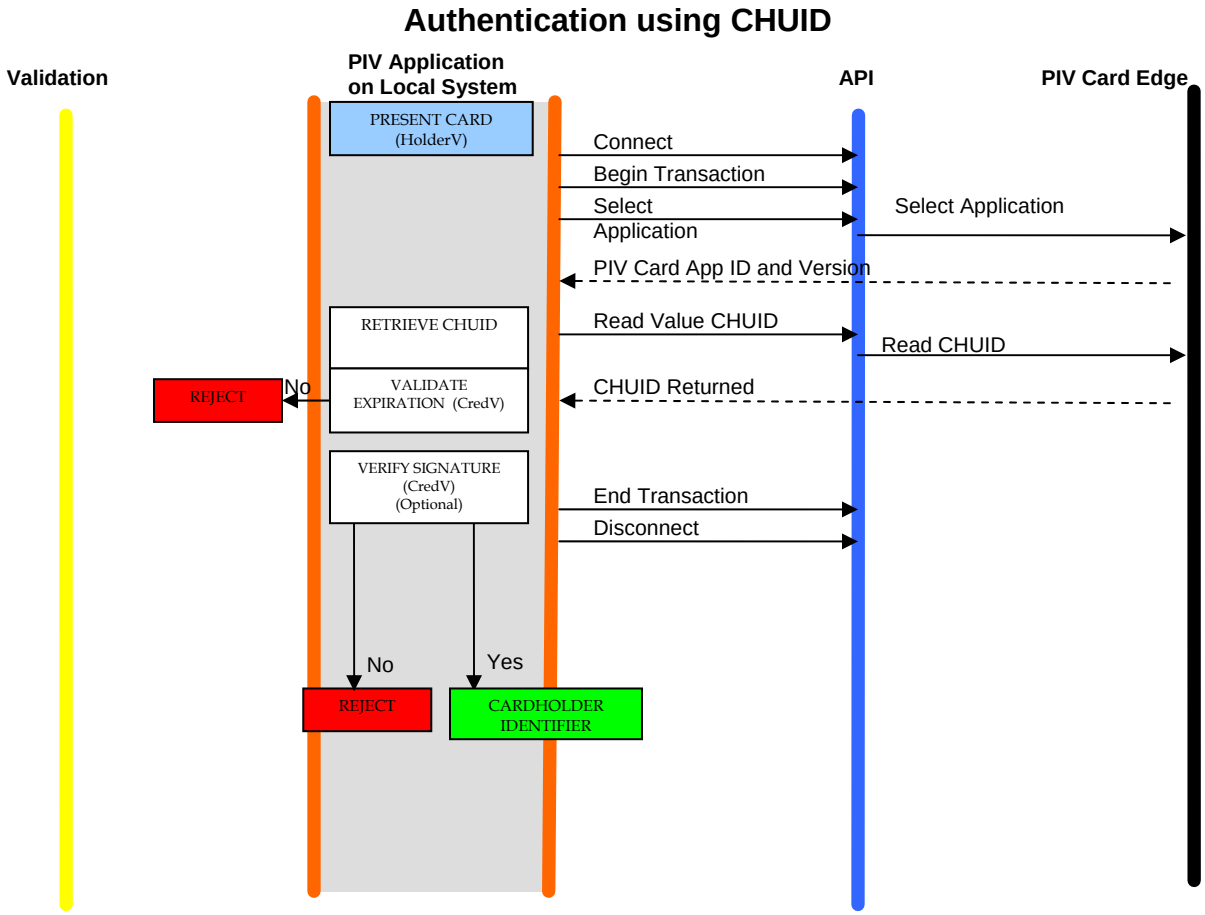

Figure B-2. Authentication using PIV CHUID

B.1.3 Authentication using PIV Biometrics

The general use case for authentication using the PIV biometric is illustrated in Figure B-4.

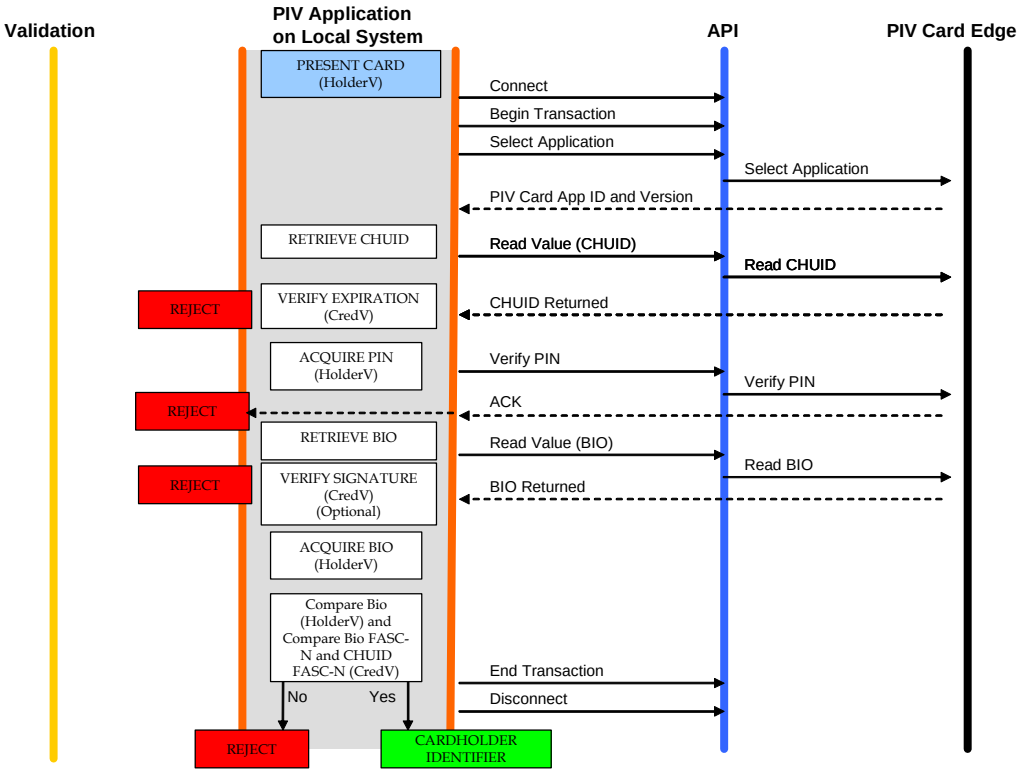

Figure B-4. Authentication using PIV Biometrics

The assurance of authentication using the PIV biometric can be further increased if the live biometric sample is collected in an attended environment, with a human overseeing the process. This use case is illustrated in Figure B-5.

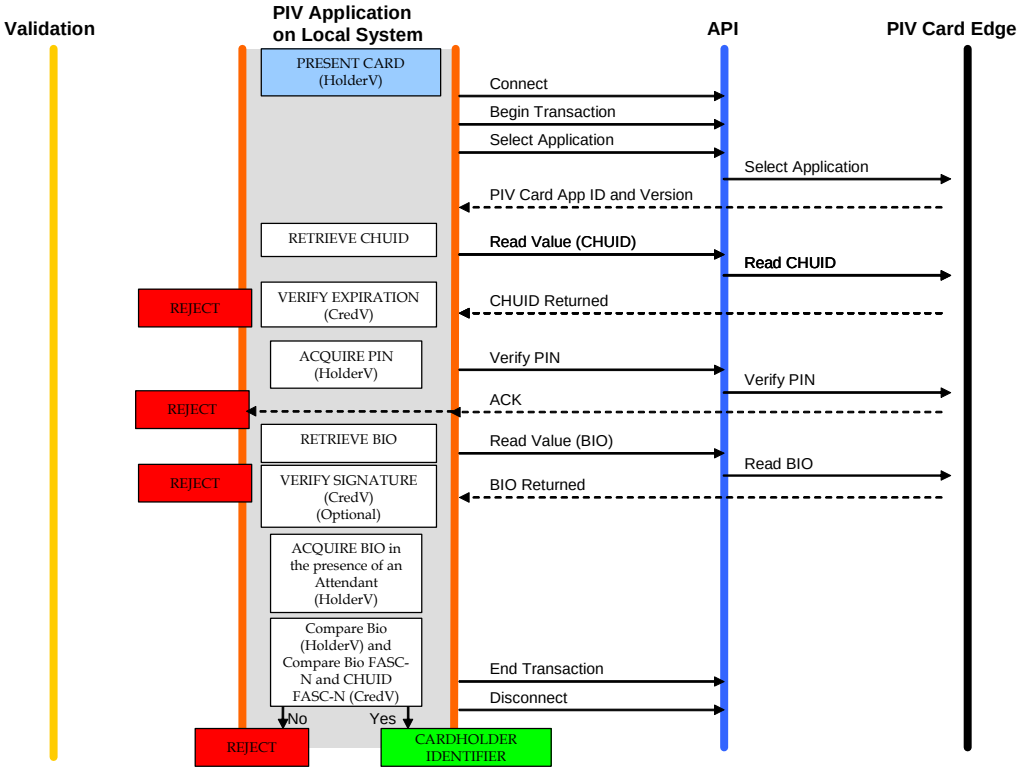

Figure B-5. Authentication using PIV Biometrics (Attended)

B.1.4 Authentication using *PIV Authentication Key*

The use case for authentication using the *PIV Authentication Key* is illustrated in Figure B-6.

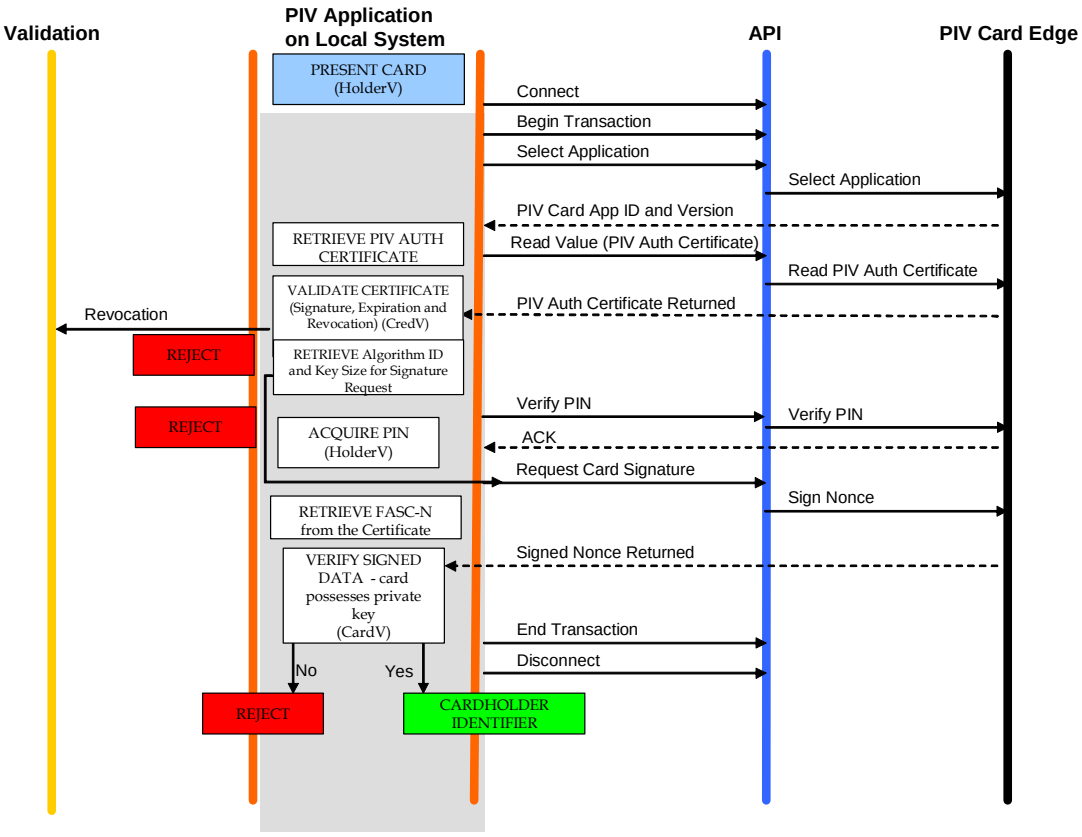

Figure B-6. Authentication using *PIV Authentication Key*

B.1.5 Authentication using Card Authentication Key

The use cases for authentication using the *Card Authentication Key* are illustrated in Figures B-7 and B-8. Figure B-7 illustrates the use-case with an asymmetric *Card Authentication Key*, while figure B-8 uses a symmetric *Card Authentication Key*. Both use cases provide "SOME" confidence in the assurance of the identity.

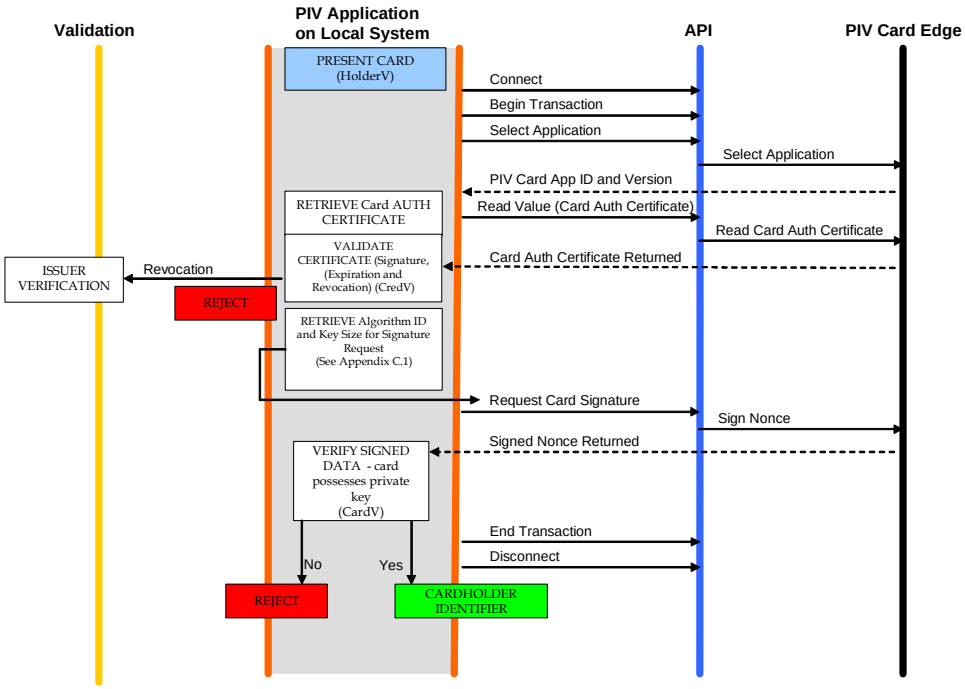

Figure B-7. Authentication using asymmetric *Card Authentication Key*

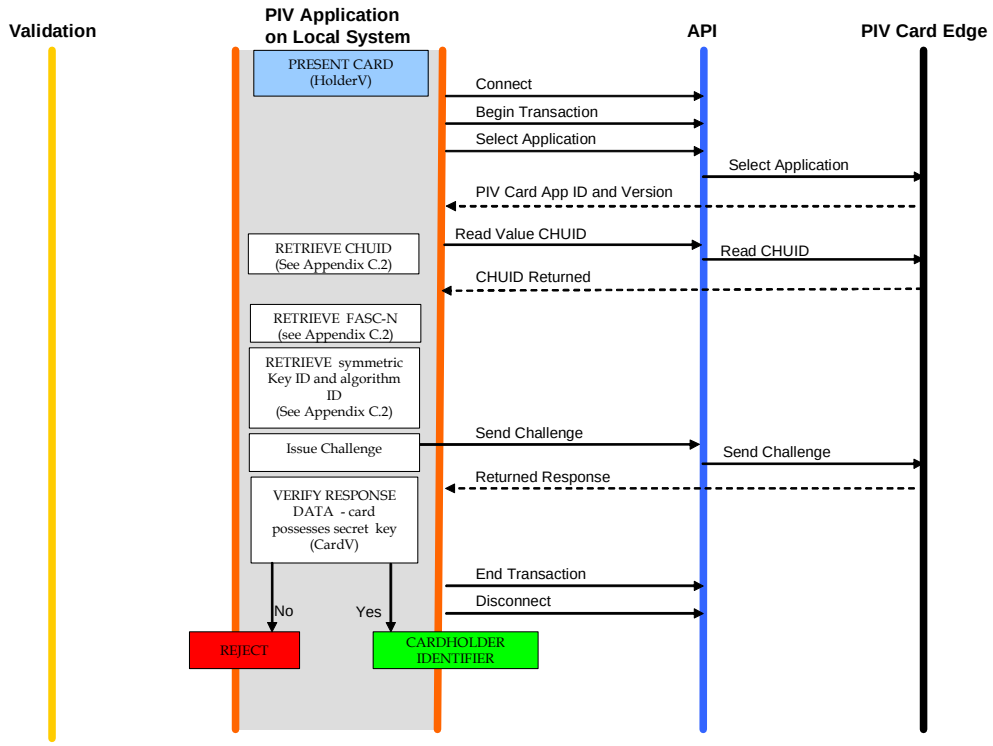

Figure B-8. Authentication using symmetric *Card Authentication Key*

B.2 Summary Table

The following table summarizes the types of validation activities that are included in each of the PIV authentication mechanisms described earlier in this section.

Table 17. Summary of PIV Authentication Mechanisms

PIV Authentication Mechanism	Card Validation Steps (CardV)	Credential Validation Steps (CredV)	Cardholder Validation Steps (HolderV)
PIV Visual Authentication	Counterfeit, tamper and forgery check	Expiration check	Possession of Card Match of card visual characteristics with cardholder
PIV CHUID		Expiration check CHUID signature check (optional)	Possession of Card
Symmetric *Card Authentication Key*	Perform challenge response with a PIV symmetric key		Possession of Card
Asymmetric *Card Authentication Key*	Perform challenge response with a PIV asymmetric Card Authentication key, and validate signature on response	Card expiration check Certificate validation of a PIV certificate	Possession of Card
PIV Authentication Key	Perform challenge response with a PIV asymmetric key, and validate signature on response	Card expiration check Certificate validation of a PIV certificate	Possession of Card Match PIN provided by Cardholder
PIV Biometric (Unattended)		Expiration check CHUID signature check (optional) PIV Bio signature check (optional) Match CHUID FASC-N with PIV Bio FASC-N	Possession of Card Match PIN provided by Cardholder Match Cardholder bio with PIV bio
PIV Biometric (Attended)		Expiration check CHUID signature check (optional) PIV Bio signature check (optional) Match CHUID FASC-N with PIV Bio FASC-N	Possession of Card Match PIN provided by Cardholder Match of Cardholder bio to PIV bio *in view of attendant*

Appendix C—PIV Algorithm Identifier Discovery

Relying Parties interact with many PIV cards with the same native key-type implemented by different key sizes and algorithms[9]. For example, a relying party performing the Authentication Use Case described in B.1.4 (Authentication using the *PIV Authentication Key*), can expect to perform a challenge and response cryptographic authentication with 1) a PIV card with RSA 1024 bit *PIV Authentication Key*, 2) a PIV card with RSA 2048 bit *PIV Authentication Key* or 3) a PIV card with an elliptic curve key (P-256) *PIV Authentication Key*.

This appendix describes recommended procedures for key size and algorithm discovery (PIV algorithm ID discovery) to facilitate cryptographic authentication initiated by the relying party to make appropriate decisions for granting access to logical networks and systems as well as physical access control systems. The discovery procedure is defined in terms of asymmetric and symmetric cryptographic authentication.

C.1 PIV Algorithm Identifier Discovery for Asymmetric Cryptographic Authentication

As illustrated in the authentication use cases in Appendix B, an asymmetric cryptographic authentication involves issuing a challenge (request to sign a nonce) to the PIV card. The relying party issuing the command provides the nonce to be signed, the PIV key reference, and the PIV algorithm identifier as parameters of the command. The nonce is random data generated by the relying party and the PIV key reference is known. The PIV algorithm identifier, on the other hand, is unknown to the relying party and needs to be identified in order to issue the challenge command. The PIV algorithm identifier can be derived from the previous steps of the authentication use case. The relying party, prior to the challenge command, retrieved and parsed the X.509 certificate from the card in order to 1) optionally validate the certificate and 2) extract the public key for the pending decryption and matching of the signed nonce once returned from the card. It is during the parsing of the X.509 certificate that the PIV algorithm identifier can be identified in two steps[10]:

Step 1: Algorithm Type Discovery:
The X.509 certificate stores the public key in the SubjectPublicKeyInfo field. The same field also stores the X.509 AlgorithmIdentifier object identifiers (OIDs). This OID identifies the algorithm (RSA, or ECC) as listed in table 3-5 of SP 800-78.

Step 2: Key Size Discovery:[11]
The public key of the certificate holder is stored in the X.509 SubjectPublicKeyInfo field. By reading the modulus n bit string, in case of a RSA key, or the Curve Point string, in case of an elliptic curve public key, the corresponding private key size is implicitly known since both public and private keys are of the same length.

[9] Table 3.1 , SP 800-78-1 list the various PIV algorithm identifiers to choose one for each PIV key type

[10] The PIV algorithm identifiers specify both the key and the algorithm for the key references, Thus both values have to be discovered in order to derive the PIV algorithm identifier

[11] If the AlgorithmIdentifier OID indicates an elliptic curve algorithm and its EcpkParameters does not indicate implicit inherited from the issuer's certificate, then the namedCurve field in the EcpkParameters encodes the curve as per table 3.6 of SP 800-78. The associated named curve, indicates the key size x of curve P-xxx. This is an alternative method to discover the key size for an elliptic curve keys.

As a final step, the discovered X.509 algorithm OID and key size is mapped to the PIV Algorithm Identifiers as defined in SP 800-78 table 6-2. The relying party then proceeds to issue the general authenticate command to the card.

C.2 PIV Algorithm Identifier Discovery for Symmetric Cryptographic Authentication

In the absence of a X.509 certificate, as is the case with symmetric cryptography, the PIV algorithm identifier discovery mechanism has to rely on a lookup table residing at the local system. The table maps a unique card identifier and key reference (inputs) to an associated PIV algorithm identifier (output). The unique identifier supplied by the card shall be Agency Code || System Code || Credential Number of the FASC-N.

The optional *card authentication key* can be a symmetric key or an asymmetric key. A relying party has no prior knowledge of 1) the key's existence and 2) the key symmetric or asymmetric implementation. The following routine discovers the *Card Authentication Key's* native implementation:

1) Attempt to read the X.509 PIV Card Authentication Certificate.
   + If the first step succeeds, the *Card Authentication Key* is asymmetric. The asymmetric PIV algorithm identifier discovery (C.1) mechanism should be followed.
   + If the first step fails, the *Card Authentication Key* a) does not exist or b) is a symmetric key.
2) Read the CHUID and extract the Agency Code || System code || Credential Number from the CHUID's FASC-N.
3) Attempt to retrieve the PIV algorithm identifier from the local lookup table.
   + If a valid PIV algorithm identifier is returned, the *Card Authentication Key* is symmetric.
   + If no algorithm identifier is returned, the PIV card does not implement the key.

Appendix D—Terms, Acronyms, and Notation

D.1 Terms

Algorithm Identifier	A PIV algorithm identifier is a one-byte identifier that specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of operation (i.e., CBC or ECB).
Application Identifier	A globally unique identifier of a card application as defined in ISO/IEC 7816-4.
Application Session	The period of time within a card session between when a card application is selected and a different card application is selected or the card session ends.
Authenticatable Entity	An entity that can successfully participate in an authentication protocol with a card application.
BER-TLV Data Object	A data object coded according to ISO/IEC 8825-2.
Card	An integrated circuit card.
Card Application	A set of data objects and card commands that can be selected using an application identifier.
Client Application	A computer program running on a computer in communication with a card interface device.
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.
Interface Device	Synonym for card interface device.
Key Reference	A PIV key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. The identifier is part of cryptographic material used in a cryptographic protocol such as an authentication or a signing protocol.
MSCUID	An optional legacy identifier included for compatibility with Common Access Card and Government Smart Card Interoperability Specifications.
Object Identifier	A globally unique identifier of a data object as defined in ISO/IEC 8824-2.
PIV Key Type	A type of a Key. The PIV Key Types are 1) PIV Authentication Key, 2) PIV Card Authentication Key, 3) PIV Digital Signature Key, 4) The PIV Key Management Key and 5) The Card Application Administration Key.
Relying Party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system.

Status Word	Two bytes returned by an integrated circuit card after processing any command that signify the success of or errors encountered during said processing.

D.2 Acronyms

AID	Application Identifier
API	Application Programming Interface
ASN.1	Abstract Syntax Notation
BER	Basic Encoding Rules
CBC	Cipher Block Chaining
CBEFF	Common Biometric Exchange Formats Framework
CCC	Card Capability Container
CHUID	Card Holder Unique IDentifier
DES	Data Encryption Standard
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
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
OID	Object Identifier
OMB	Office of Management and Budget
PACS	Physical Access Control System
PIN	Personal Identification Number
PIV	Personal Identity Verification
PIX	Proprietary Identifier eXtension
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key
RFU	Reserved for Future Use
RID	Registered application provider IDentifier
RSA	Rivest, Shamir, Aldeman
SCEPACS	Smart Card Enabled Physical Access Control System
SCP	ETSI Smart Card Project
SP	Special Publication
SW1	First byte of a two-byte status word
SW2	Second byte of a two-byte status word
TIG	Technical Implementation Guidance
TLV	Tag-Length-Value
URL	Uniform Resource Locator

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

BER-TLV data object tags are represented as byte sequences as described above. Thus, for example, ‘4F’ is the interindustry data object tag for an application identifier and ‘7F 60’ is the interindustry data object tag for the biometric information template.

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 [8].

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

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

[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] *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.

[6] ISO/IEC 8824-2:2002, *Information technology -- Abstract Syntax Notation One (ASN.1): Information object specification.*

[7] ISO/IEC 8825-1:2002, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).*

[8] NIST Special Publication 800-78-1, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, May 2007. (See http://csrc.nist.gov)

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