Revised Draft NIST Special Publication 800-73-4

Formatted

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

Ramaswamy Chandramouli
David Cooper
Hildegard Ferraiolo
Salvatore Francomacaro
Ketan Mehta
Jason Mohler

COMPUTER SECURITY

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

Revised Draft NIST Special Publication 800-73-4

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

Ramaswamy Chandramouli
David Cooper
Hildegard Ferraiolo
Salvatore Francomacaro
Ketan Mehta
Computer Security Division
Information Technology Laboratory

Jason Mohler
Electrosoft Services, Inc.

May 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Revised Draft Special Publication 800-73-4 Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline 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 Circular A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided in Circular A-130, Appendix III, Security of Federal Automated Information Resources.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-73-4
Natl. Inst. Stand. Technol. Spec. Publ. 800-73-4, 64 pages (May 2014)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *May 16, 2014* through *June 16, 2014*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv_comments@nist.gov

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 other than national security-related information in Federal information systems. The 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.

Abstract

FIPS 201 defines the requirements and characteristics of a government-wide interoperable identity credential. FIPS 201 also specifies that this identity credential must be stored on a smart card. This document, SP 800-73, contains the technical specifications to interface with the smart card to retrieve and use the PIV 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, this document enumerates requirements where the international integrated circuit card standards [ISO7816] 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.

Keywords

authentication; FIPS 201; identity credential; logical access control; on-card biometric comparison; Personal Identity Verification (PIV); physical access control; smart cards; secure messaging

Acknowledgements

The authors (Ramaswamy Chandramouli, David Cooper, Hildegard Ferraiolo, Salvatore Francomacaro, and Ketan Mehta of NIST, and Jason Mohler of Electrosoft Services, Inc.) wish to thank their colleagues who reviewed drafts of this document and contributed to its development. 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.

I. Revision History

Version	Release Date	Updates
SP 800-73	April 2005	Initial Release
SP 800-73-1	April 2006	Incorporated Errata
SP 800-73-2	September 2008	• Separated SP 800-73 into four Parts: 1 - *End-Point PIV Card Application Namespace, Data Model and Representation* *2 - End-Point PIV Card Application Card Command Interface* *3 - End-Point PIV Client Application Programming Interface* *4 - The PIV Transitional Interface and Data Model Specification* • All PIV cryptographic key types, cryptographic algorithm identifiers, and key sizes previously listed in SP 800-73-1, are now specified in SP 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification* • Removed default algorithms. Each PIV key type can be implemented from a small subset of algorithms and key sizes as specified in Table 3-1 of SP 800-78 • Added optional Discovery Object (Part 1, Section 3.2.6) • Added optional capability to use the Global PIN (in addition to the PIV Card Application PIN) with the PIV Card Application (Part 1, Section 3.2.6) • Added pivMiddlewareVersion API function (Part 3, Section 3.1.1) • Deprecated the CHUID data object's Authentication Key Map data element • Deprecated the Printed Information data object's Employee Affiliation Line 2 data element (tag 0x03) • Removed size limits on signed data object containers (Part 1, Appendix A)
SP 800-73-3	February 2010	• Added preamble: I - Revision History, II - Configuration Management and III – NPIVP Conformance Testing. (Part 1, Preamble) • Removed the CHUID data object's Authentication Key Map data element • Removed the Printed Information data object's Employee Affiliation Line 2 data element (tag 0x03) • Deprecated IPv6 as optional value for the CHUID's GUID data element (Part 1, Section 3.2.1) • Added Key History capability (Part 1, Section 3.2.7) • Added ECDH key agreement scheme (Part 2, Section 3.2.4) • Added UUID feature for non-Federal issuer cards (Part 1, Section 3.3) • Expanded Part 2, Appendix A (GENERAL AUTHENTICATE examples) to illustrate ECDSA signatures and key establishment schemes with the key management key • Added an optional cardholder iris images data object, which is specified in SP 800-76-2. • Added Appendix C, PIV Algorithm Identifier Discovery. • Updated PIV Middleware version number in Part 3.

Deleted: NFI

Deleted: will be

Revised Draft Special Publication 800-73-4 Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation

Version	Release Date	Updates
SP 800-73-4	May 2014	• Removed Part 4, The PIV Transitional Data Model and Interfaces • Removed “End-Point” from the titles and content of Parts 1 through 3 • Added Section 1.3 “Effective Date” • Made asymmetric Card Authentication key mandatory • Made digital signature key and key management key conditionally mandatory • Made the facial image data object mandatory • Introduced specifications for optional secure messaging • Introduced specifications for optional virtual contact interface (VCI) over which all non-card-management functionality of the PIV Card is accessible • Added support for pairing code that is used to establish VCI • Made Card UUID mandatory. Thus, removed the option to populate the GUID data element of CHUID with all zeros or an IPv6 address • Added PIV card level PIN length enforcement requirements for the PINs • Added an optional Cardholder UUID as a unique identifier for a cardholder • Removed information about encoding of NFI cards • Added optional on-card biometric comparison mechanism as a means of performing card activation and as a PIV authentication mechanism • Added requirement for signature verification and certification path validation in the CHUID, BIO, and BIO-A authentication mechanisms • Added the On Card Comparison (OCC) Biometric Information (BIT) group template Data Object • Added Secure Messaging Signer Certificate Data Object • Added Pairing Code Reference Data Container • Deprecated some data elements in the CHUID (Buffer Length, DUNS and Organization Identifier) and legacy data elements in all X.509 Certificates (MSCUID) • Deprecated the optional Extended Application CardURL and Security Object Buffer data elements from the Card Capability Container • Updated PIV Middleware version number in Part 3 • Expanded Part 1, Appendix C (PIV Algorithm Identifier Discovery) to include an Algorithm Identifier discovery for Secure Messaging • Expanded Part 2, Appendix A (GENERAL AUTHENTICATE examples) to illustrate use of VCI

Deleted: optional

Deleted: virtual contact interface

Deleted: d

Deleted: , pairing code and PUK

II. Configuration Management

When a Federal agency adds one or several optional features listed in the previous section (Revision History) to its PIV Cards, it is necessary for client applications to upgrade the PIV Middleware accordingly. This will enable the PIV Middleware to recognize and process the new data objects and/or features.

Deleted: their

Where maximum interoperability is required, it is necessary to upgrade to SP 800-73-4 based PIV Middleware as they become available. Only SP 800-73-4 based PIV Middleware fully support all capabilities outlined in the Revision History.[1] Previous versions of the PIV Middleware (based on SP800-73-3, SP 800-73-2, or SP 800-73-1) are unaware of new SP 800-73-4 features and thus have the following limitations:

- SP 800-73-3 based PIV Middleware:
    - Do not support On-card Biometric Comparison
    - Do not support Secure Messaging.

    Recommendation: SP 800-73-3 based PIV Middleware should be restricted to applications that do not use the above features.

- In addition to the limitations listed above, SP 800-73-2 based PIV Middleware:
    - Do not support the Key History feature.
    - Do not support the iris images data object.

    Recommendation: SP 800-73-2 based PIV Middleware should be restricted to applications that do not use the new features supported by the SP 800-73-3 and SP 800-73-4 middleware.

- In addition to the limitations listed above, SP 800-73-1 based PIV Middleware:
    - Do not recognize the PIV Discovery Object and thus are unable to recognize or prompt for the Global PIN for PIV Cards with Global PIN enabled.
    - Do not support the PIV Middleware version API function.

    Recommendation: SP 800-73-1 based PIV Middleware should be restricted to applications that do not use the new features supported by the SP 800-73-2, SP 800-73-3, and SP 800-73-4 middleware.

[1] Implementation of secure messaging and virtual contact interface are optional.

III NPIVP Conformance Testing

As outlined in FIPS 201-2, Appendix A.3, NIST has established the NIST Personal Identity Verification Program (NPIVP) to:

+ validate the compliance/conformance of two PIV components: PIV Middleware and PIV Card Applications with the specifications in NIST SP 800-73 and
+ provide the assurance that the set of PIV Middleware and PIV Card Applications that have been validated by NPIVP are interoperable.

For the further information on NPIVP, see http://csrc.nist.gov/groups/SNS/piv/npivp/index.html.

With the final release of SP 800-73-4, NPIVP plans to revise and publish SP 800-85A-3, PIV Card Application and Middleware Interface Test Guidelines. This document will outline the Derived Test Requirements (DTRs) of SP 800-73-4 based PIV Card Applications and PIV Middleware. In parallel, NPIVP plans to update the test tools for NPIVP laboratories to test PIV Card Applications and PIV Middleware in accordance with the DTRs in SP 800-85A-3. Once SP 800-85A-3 is published, and the test tools are available to NPIVP test laboratories, SP 800-73-3 based testing will be discontinued and SP 800-73-4 based testing will begin. NPIVP will announce the start of SP 800-73-4 based testing at http://csrc.nist.gov/groups/SNS/piv/npivp/announcements.html.

Table of Contents

I. REVISION HISTORY IV
II. CONFIGURATION MANAGEMENT VI
III NPIVP CONFORMANCE TESTING VII
1. INTRODUCTION 1
1.1 PURPOSE 1
1.2 SCOPE 1
1.3 EFFECTIVE DATE 1
1.4 AUDIENCE AND ASSUMPTIONS 2
1.5 DOCUMENT OVERVIEW AND STRUCTURE 2
2. PIV CARD APPLICATION NAMESPACES 3
2.1 NAMESPACES OF THE PIV CARD APPLICATION 3
2.2 PIV CARD APPLICATION AID 3
3. PIV DATA MODEL ELEMENTS 4
3.1 MANDATORY DATA ELEMENTS 4
3.1.1 Card Capability Container 4
3.1.2 Card Holder Unique Identifier 5
3.1.3 X.509 Certificate for PIV Authentication 7
3.1.4 X.509 Certificate for Card Authentication 7
3.1.5 Cardholder Fingerprints 7
3.1.6 Cardholder Facial Image 7
3.1.7 Security Object 7
3.2 CONDITIONAL DATA ELEMENTS 8
3.2.1 X.509 Certificate for Digital Signature 8
3.2.2 X.509 Certificate for Key Management 8
3.3 OPTIONAL DATA ELEMENTS 9
3.3.1 Printed Information 9
3.3.2 Discovery Object 9
3.3.3 Key History Object 10
3.3.4 Retired X.509 Certificates for Key Management 12
3.3.5 Cardholder Iris Images 12
3.3.6 Biometric Information Templates Group Template 12
3.3.7 Secure Messaging Certificate Signer 12
3.3.8 Pairing Code Reference Data Container 13
3.4 INCLUSION OF UNIVERSALLY UNIQUE IDENTIFIERS (UUIDS) 13
3.4.1 Card UUID 13
3.4.2 Cardholder UUID 13
3.5 DATA OBJECT CONTAINERS AND ASSOCIATED ACCESS RULES AND INTERFACE MODES 14
4. PIV DATA OBJECTS REPRESENTATION 16
4.1 DATA OBJECTS DEFINITION 16
4.1.1 Data Object Content 16
4.2 OIDS AND TAGS OF PIV CARD APPLICATION DATA OBJECTS 16
4.3 OBJECT IDENTIFIERS 16
5. DATA TYPES AND THEIR REPRESENTATION 18
5.1 KEY REFERENCES 18
5.1.1 OCC Data 20
5.1.2 PIV Secure Messaging Key 20
5.1.3 Pairing Code 20
5.2 PIV ALGORITHM IDENTIFIER 21
5.3 CRYPTOGRAPHIC MECHANISM IDENTIFIERS 21

5.4 Secure Messaging 21
5.5 Virtual Contact Interface 21
5.6 Status Words 22

LIST OF APPENDICES

Appendix A— PIV Data Model 23

Appendix B— PIV Authentication Mechanisms 35

B.1 Authentication Mechanism Diagrams 36
B.1.1 Authentication Using PIV Biometrics (BIO) 37
B.1.2 Authentication Using PIV Authentication Key 39
B.1.3 Authentication Using Card Authentication Key 40
B.1.4 Authentication Using OCC (OCC-AUTH) 42
B.1.5 Authentication Using PIV Visual Credentials 43
B.1.6 Authentication Using PIV CHUID 44
B.2 Summary Table 45

Appendix C— PIV Algorithm Identifier Discovery 46

C.1 PIV Algorithm Identifier Discovery for Asymmetric Cryptographic Authentication 46
C.2 PIV Algorithm Identifier Discovery for Symmetric Cryptographic Authentication 47
C.3 PIV Algorithm Identifier Discovery for Secure Messaging 47

Appendix D— Terms, Acronyms, and Notation 48

D.1 Terms 48
D.2 Acronyms 49
D.3 Notation 51

Appendix E— References 52

LIST OF TABLES

Table 1. First Byte of PIN Usage Policy Discovery 9

Table 2. Data Model Containers 14

Table 3. Object Identifiers of the PIV Data Objects for Interoperable Use 17

Table 4. PIV Card Application Authentication and Key References 18

Table 5. Cryptographic Mechanism Identifiers 21

Table 6. Status Words 22

Table 7. PIV Data Containers 23

Table 8. Card Capability Container 25

Table 9. Card Holder Unique Identifier 26

Table 10. X.509 Certificate for PIV Authentication 26

Table 11. Cardholder Fingerprints 26

Table 12. Security Object 27

Table 13. Cardholder Facial Image 27

Table 14. Printed Information 27

Table 15. X.509 Certificate for Digital Signature 27

Table 16. X.509 Certificate for Key Management 28

Table 17. X.509 Certificate for Card Authentication 28
Table 18. Discovery Object 28
Table 19. Key History Object 28
Table 20. Retired X.509 Certificate for Key Management 1 29
Table 21. Retired X.509 Certificate for Key Management 2 29
Table 22. Retired X.509 Certificate for Key Management 3 29
Table 23. Retired X.509 Certificate for Key Management 4 29
Table 24. Retired X.509 Certificate for Key Management 5 30
Table 25. Retired X.509 Certificate for Key Management 6 30
Table 26. Retired X.509 Certificate for Key Management 7 30
Table 27. Retired X.509 Certificate for Key Management 8 30
Table 28. Retired X.509 Certificate for Key Management 9 31
Table 29. Retired X.509 Certificate for Key Management 10 31
Table 30. Retired X.509 Certificate for Key Management 11 31
Table 31. Retired X.509 Certificate for Key Management 12 31
Table 32. Retired X.509 Certificate for Key Management 13 32
Table 33. Retired X.509 Certificate for Key Management 14 32
Table 34. Retired X.509 Certificate for Key Management 15 32
Table 35. Retired X.509 Certificate for Key Management 16 32
Table 36. Retired X.509 Certificate for Key Management 17 33
Table 37. Retired X.509 Certificate for Key Management 18 33
Table 38. Retired X.509 Certificate for Key Management 19 33
Table 39. Retired X.509 Certificate for Key Management 20 33
Table 40. Cardholder Iris Images 34
Table 41. Biometric Information Templates Group Template 34
Table 42. Secure Messaging Certificate Signer 34
Table 43. Pairing Code Reference Data Container 34
Table 44. Summary of PIV Authentication Mechanisms 45

LIST OF FIGURES

Figure B-1. Authentication using PIV Biometrics (BIO) 37
Figure B-2. Authentication using PIV Biometrics Attended (BIO-A) 38
Figure B-3. Authentication using PIV Authentication Key 39
Figure B-4. Authentication using an asymmetric Card Authentication Key 40
Figure B-5. Authentication using a symmetric Card Authentication Key 41
Figure B-6. Authentication using OCC 42
Figure B-7. Authentication using PIV Visual Credentials 43
Figure B-8. Authentication using PIV CHUID 44

1. Introduction

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 Federally controlled facilities and information systems. Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201 (FIPS 201) [FIPS201] was developed to establish standards for identity credentials. Special Publication 800-73-4 (SP 800-73-4) contains technical specifications to interface with the smart card (PIV Card[2]) to retrieve and use the identity credentials.

1.1 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 800-73-4 contains the 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, this document enumerates requirements where the international integrated circuit card standards [ISO7816] 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.

1.2 Scope

SP 800-73-4 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 described 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 interchangeably by all information processing systems across Federal agencies. SP 800-73-4 defines the PIV data elements' identifiers, structure, and format. SP 800-73-4 also describes the client application programming interface and card command interface for use with the PIV Card.

This part, SP 800-73-4, Part 1 – *PIV Card Application Namespace, Data Model and Representation*, specifies the PIV Card Application Namespace, the PIV Data Model and its logical representation on the PIV Card, and is a companion document to FIPS 201.

1.3 Effective Date

Federal departments and agencies may implement these recommendations, rather than the previous version, immediately upon publication. With the exception of the requirement for the PIV Card Application to enforce the minimum length requirements for the PINs, Federal

Deleted: , paring code, and PIN Unblocking Key (PUK)

[2] A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains a PIV Card Application which stores identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) 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).

departments and agencies must implement these recommendations no later than 12 months after the effective date of FIPS 201-2.

The requirement to enforce minimum length for the PINs at the card level is a security requirement that did not appear in previous versions of SP 800-73. The implementation schedule for this new requirement shall be phased in as part of new card stock acquisition by Federal departments and agencies after final publication of this document.

Deleted: , pairing code, and PUK,

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:

- Section 1, *Introduction*, provides the purpose, scope, effective date, audience, and assumptions, of the document and outlines its structure.
- Section 2, *PIV Card Application Namespaces*, defines the three NIST managed namespaces used by the PIV Card Application.
- Section 3, *PIV Data Model Elements*, describes the PIV Data Model elements in detail.
- Section 4, *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, *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.
- Appendix A provides container information of PIV Cards and is normative. All other appendices are informative and contain material that needs special formatting together with illustrative material to aid in understanding information in the body of the document.

Deleted: The

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 (PIX) of the NIST Registered Application Provider IDentifier (RID)
- ASN.1 object identifiers (OIDs) in the personal identity 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* [ISO7816], and used in the NIST coexistent tag allocation scheme without redefinition have the same meaning as they have in [ISO7816].

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 first version of the PIV Card Application. All other PIX sequences on the NIST RID 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. 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 seven mandatory interoperable data objects, two conditionally mandatory data objects, and may contain twenty-seven optional data objects. The seven mandatory data objects for interoperable use are as follows:

Deleted: four

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

The two data objects that are mandatory if the cardholder has a government-issued email account at the time of credential issuance are:

1. X.509 Certificate for Digital Signature
2. X.509 Certificate for Key Management

The twenty-seven optional data objects are as follows:

Deleted: four

1. Printed Information
2. Discovery Object
3. Key History Object
4. 20 retired X.509 Certificates for Key Management
5. Cardholder Iris Images
6. Biometric Information Templates Group Template
7. Secure Messaging Certificate Signer
8. Pairing Code Reference Data Container

3.1 Mandatory Data Elements

This section describes the seven mandatory data objects for interagency interoperable use.

3.1.1 Card Capability Container

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

The CCC supports minimum capability for retrieval of the data model and optionally the application information as specified in [GSC-IS]. 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 PIV Card Applications, the PIV data objects exist in a namespace tightly managed by NIST and a CCC discovery mechanism is not needed by client applications that are not based on GSC-IS. Therefore, all mandatory 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). Unused optional data elements shall be absent. The content of the CCC data elements, other than the data model number, are out of scope for this specification.

3.1.2 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) [TIG SCEPACS]. For this specification, the CHUID is common between the contact and contactless interfaces. 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 optional Buffer Length TLV element is deprecated and will be eliminated in a future version of SP 800-73. 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.

Deleted: field is an optional

Deleted: .

Deleted: This

- The previously deprecated Authentication Key Map data element shall not be present in the CHUID.[3]

- The Federal Agency Smart Credential Number (FASC-N) shall be in accordance with TIG SCEPACS [TIG SCEPACS] with the exception that credential series, individual credential issue, person identifier, organizational category, organizational identifier, and person/organization association category may be populated with all zeros.

  A subset of the FASC-N, the FASC-N Identifier, shall be the unique identifier as described in [TIG SCEPACS, Section 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 SP 800-87, *Codes for Identification of Federal and Federally-Assisted Organizations* [SP800-87]. 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 the 10th paragraph of [TIG SCEPACS, Section 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."

Deleted: set to

- The optional DUNS and Organizational Identifier fields are deprecated and will be eliminated in a future version of SP 800-73.

Deleted: Code

Deleted: are optional

[3] See Revision History in preamble of this document.

[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 shall include a Card Universally Unique Identifier (UUID) (see Section 3.4.1).
- 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 in ASCII as YYYYMMDD. The expiration date shall be the same as printed on the card.
- The optional Cardholder UUID field is mapped to RFU tag 0x36. If present, it shall include a Cardholder UUID as described in Section 3.4.2.
- The CHUID shall be signed in accordance with Section 3.1.2.1. 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.

Deleted: Unique Identification Number

3.1.2.1 Asymmetric Signature Field in CHUID

FIPS 201 requires inclusion of the asymmetric signature field in the CHUID data object. The asymmetric signature data element of the CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as defined in RFC 5652 [RFC5652].

The issuer asymmetric signature field is implemented as a *SignedData* type, as specified in [RFC5652], and shall include the following information:

- The message shall include a *version* field specifying version v3
- The *digestAlgorithms* field shall be as specified in [SP800-78]
- The *encapContentInfo* shall:
  - Specify an *eContentType* of id-PIV-CHUIDSecurityObject
  - Omit the *eContent* field
- The *certificates* field shall include only a single X.509 certificate, which can be used to verify the signature in the *SignerInfo* field
- The *crls* field shall be omitted
- *signerInfo*s shall be present and include only a single *SignerInfo*
- The *SignerInfo* shall:
  - Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
  - Specify a *digestAlgorithm* in accordance with [SP800-78]
  - Include, at a minimum, the following signed attributes:
    - A *MessageDigest* attribute containing the hash computed in accordance with [SP800-78]
    - A *pivSigner-DN* attribute containing the subject name that appears in the PKI certificate for the entity that signed the CHUID
  - Include the digital signature.

The public key required to verify the digital signature shall be provided in the *certificates* field in an X.509 digital signature certificate that has been issued in accordance with Section 4.2.1 of FIPS 201-2.

3.1.3 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 PIV Authentication private key and its corresponding certificate are only available over the contact interface or Virtual Contact Interface (VCI). 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 4) is protected with a Personal Identification Number (PIN) or On-Card biometric Comparison (OCC) access rule. In other words, private key operations using the PIV Authentication key require the PIN or OCC data to be submitted and verified, but a successful submission enables multiple private key operations without additional cardholder consent.

3.1.4 X.509 Certificate for Card Authentication

FIPS 201 specifies the mandatory asymmetric Card Authentication key (CAK) as a private key that may be used to support physical access applications. 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. The PKI cryptographic function (see Table 4) is under an "Always" access rule, and thus private key operations can performed without access control restrictions. The asymmetric CAK is generated by the PIV Card Issuer in accordance with FIPS 140-2 requirements for key generation. An asymmetric CAK may be generated on-card or off-card. If an asymmetric CAK is generated off-card, the result of each key generation shall be injected into at most one PIV Card.

Deleted: protected with

Deleted: . In other words

3.1.5 Cardholder Fingerprints

The fingerprint data object specifies the primary and secondary fingerprints for off-card matching in accordance with FIPS 201 and SP 800-76.

3.1.6 Cardholder Facial Image

The facial image data object supports visual authentication by a guard, and may also be used for automated facial authentication in operator-attended PIV issuance, reissuance, and verification data reset processes. The facial image data object shall be encoded as specified in [SP800-76].

3.1.7 Security Object

The Security Object is in accordance with Appendix 3 to Section IV of Volume 2 of Part 3 of Machine Readable Travel Documents (MRTD) [MRTD]. 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.

Deleted: C

Deleted: PKI for

Deleted: Offering ICC Read-Only Access Version 1.1

The "DG-number-to-Container-ID" mapping object TLV in tag 0xBA encapsulates a series of three-byte sequences – 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 [MRTD, Appendix 3 to Section IV]. The Logical Data Structure (LDS) Security Object itself must be in ASN.1 DER format, formatted as specified in [MRTD, Appendix A.3.2]. This structure is then inserted into the *encapContentInfo* field of the Cryptographic Message Syntax (CMS) object specified in [MRTD, Appendix A.3.1].

Deleted: C

Deleted: C

Deleted: C

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 and the Secure Messaging Certificate Signer data object, be included in the Security Object.

3.2 Conditional Data Elements

The following two data elements are mandatory if the cardholder has a government-issued email account at the time of credential issuance. These two data elements, when implemented, shall conform to the specifications provided in this document.

3.2.1 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 digital signature private key and its corresponding certificate are only available over the contact interface or VCI. The read access control rule for the X.509 Certificate for Digital Signing is "Always," meaning the certificate can be read without access control restrictions. The PKI cryptographic function (see Table 4) is protected with a "PIN Always" or "OCC Always" access rule. In other words, the PIN or OCC data must be submitted and verified every time immediately before a *digital signature key* operation. This ensures cardholder participation every time the private key is used for digital signature generation.[5]

3.2.2 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. The key management private key and its corresponding certificate are only available over the contact interface or VCI. 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 (see Table 4) is protected with a "PIN" or "OCC" access rule. In other words, once the PIN or OCC data is submitted and verified, subsequent *key management key* operations can be performed without requiring the PIN or OCC data again. This enables multiple private key operations without additional cardholder consent.

[5] [NISTIR7863], *Cardholder Authentication for the PIV Digital Signature Key*, addresses the appropriate use of PIN caching related to digital signatures.

3.3 Optional Data Elements

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

Deleted: four

3.3.1 Printed Information

All FIPS 201 mandatory information printed on the card is duplicated on the chip in this data object. The printed information data object shall not be modified post-issuance. 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.

3.3.2 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 mandatory 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.

Deleted: The Discovery Object may optionally include tag 0x7F61, the Biometric Information Templates (BIT) group template, and tag 0x5F50, the Uniform Resource Locator (URL).

+ 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: Bit 7 indicates whether the PIV Card Application PIN satisfies the PIV Access Control Rules (ACRs) for command execution[6] and data object access. Bit 7 shall always be set to 1.

  Bit 6 indicates whether the optional Global PIN satisfies the PIV ACRs for command execution and PIV data object access.

  Bit 5 indicates whether the optional pairing code is implemented.

  Bit 4 indicates whether the optional OCC satisfies the PIV ACRs for command execution and PIV data object access

  Bits 8 and 3 through 1 of the first byte shall be set to zero.

Deleted: 4

Table 1. First Byte of PIN Usage Policy Discovery

Value	Definition
0x40	PIV Card Application PIN alone satisfies the PIV ACRs. Pairing code has not been implemented.
0x48	Both the PIV Card Application PIN and OCC satisfy the PIV ACRs. Pairing code has not been implemented.
0x50	PIV Card Application PIN alone satisfies the PIV ACRs. Pairing code has been implemented.

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

Value	Definition
0x58	Both the PIV Card Application PIN and OCC satisfy the PIV ACRs. Pairing code has been implemented.
0x60	Both PIV Card Application PIN and Global PIN satisfy PIV ACRs. Pairing code has not been implemented.
0x68	PIV Card Application PIN, Global PIN, and OCC all satisfy PIV ACRs. Pairing code has not been implemented.
0x70	Both PIV Card Application PIN and Global PIN satisfy PIV ACRS. Pairing code has been implemented.
0x78	PIV Card Application PIN, Global PIN, and OCC all satisfy PIV ACRs. Pairing code has been implemented.

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.

PIV Card Applications that implement the pairing code shall implement the Discovery Object with the first byte of the PIN Usage Policy set to 0x50, 0x58, 0x70, or 0x78. PIV Card Applications for which both the PIV Card Application PIN and the Global PIN satisfy the PIV ACRs for PIV data object access and command execution shall implement the Discovery Object with the PIN Usage Policy set to 0x60 zz, 0x68 zz, 0x70 zz, or 0x78 zz where zz is either 0x10 or 0x20. PIV Card Applications for which OCC satisfies the PIV ACRs for PIV data object access and command execution shall implement the Discovery Object with the first byte of the PIN Usage Policy set to 0x48, 0x58, 0x68, or 0x78.

Note: If the first byte is set to 0x40, 0x48, 0x50, or 0x58, then the second byte is RFU and shall be set to 0x00.

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.

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

3.3.3 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.[7] 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

[7] See NIST Interagency Report 7676 [IR7676] for suggestions on the implementation and use of the Key History mechanism.

Deleted: 0

Deleted: 0

Deleted: 0

Deleted: <#>Tag 0x7F61 encodes the configuration information of the OCC data. The encoding of the BIT group template shall be as specified in Table 7 of [SP 800-76-2]. This tag shall be absent if OCC does not satisfy the PIV ACRs for command execution and data object access. The Discovery Object shall be implemented and tag 0x7F61 shall be present when OCC satisfies the PIV ACRs for PIV data objects access and command execution.¶
<#>Tag 0x5F50 contains an HTTP URL [RFC2616] that specifies the location of the content signing certificate needed to verify the signature on the PIV Card's card verifiable certificate (see Section 5.1.2). The location specified by the URL shall contain exactly one certificate, encoded in DER format, in accordance with [RFC2585]. The Discovery Object shall be implemented and tag 0x5F50 shall be present if the PIV Card supports secure messaging.¶

Deleted: if the card does not support either OCC or secure messaging

Deleted: The encoding of the 0x7E Discovery Object is as follows if OCC and secure messaging are supported by the card:¶
{'7E L1' {'4F 0B A0 00 00 03 08 00 00 10 00 01 00'} {'5F 2F 02 xx yy'} {'7F 61 L2 …'} {'5F 50 L3 …'}}, where xx and yy encode the first and second byte of the PIN Usage Policy as described in this section and L1, L2, and L3 provide the lengths of '7E', '7F 61', and '5F 50' respectively.¶

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 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 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.

[8] The ASN.1 for **Certificate** may be imported from the ASN.1 module **PKIX1Explicit88** in Appendix A.1 of [RFC5280].

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

Deleted: virtual contact interfaces (

Deleted:)

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

3.3.4 Retired X.509 Certificates for Key Management

These objects hold the X.509 Certificates for Key Management corresponding to retired key management private keys, as described in Section 3.3.3. Retired key management private keys and their corresponding certificates are only available over the contact interface or VCI. The read access control rule for these certificates is "Always," meaning the certificates can be read without access control restrictions. The PKI cryptographic function (see Table 4) for all of the retired key management private keys is protected with a "PIN" or "OCC" access rule. In other words, once the PIN or OCC data is submitted and verified, subsequent key management key operations can be performed with any of the retired key management private keys without requiring the PIN or OCC data again. This enables multiple private key operations without additional cardholder consent.

3.3.5 Cardholder Iris Images

The iris images data object specifies compact images of the cardholder's irises. The images are suitable for use in iris recognition systems for automated identity verification. The iris images data object shall be encoded as specified in [SP800-76].

3.3.6 Biometric Information Templates Group Template

The Biometric Information Templates (BIT) Group Template data object encodes the configuration information of the OCC data. The encoding of the BIT group template shall be as specified in Table 7 of [SP800-76]. This data object shall be absent if OCC does not satisfy the PIV ACRs for command execution and data object access. When OCC satisfies the PIV ACRs for PIV data objects access and command execution both the Discovery Object and the BIT Group Template data object shall be present, and bit 4 of the first byte of the PIN Usage Policy shall be set.

3.3.7 Secure Messaging Certificate Signer

The Secure Messaging Certificate Signer data object, which shall be present if the PIV Card supports secure messaging for non-card-management operations, contains the certificate(s) needed to verify the signature on the secure messaging card verifiable certificate (CVC), as specified in Part 2, Section 4.1.5.

The public key required to verify the digital signature of the secure messaging CVC is an ECC key. It shall be provided in either an X.509 Certificate for Content Signing or an Intermediate CVC. If the public key required to verify the digital signature of the secure messaging CVC is provided in an Intermediate CVC, then the format of the Intermediate CVC shall be as specified in Part 2, Section 4.1.5, and the public key required to verify the digital signature of the Intermediate CVC shall be provided in an X.509 Certificate for Content Signing.

The X.509 Certificate for Content Signing shall be a digital signature certificate issued under the id-fpki-common-piv-contentSigning policy of [COMMON]. The X.509 Certificate for Content Signing shall also include an extended key usage (*extKeyUsage)* extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix B of FIPS 201-2. The

X.509 Certificate for Content Signing needed to verify the digital signature of a secure messaging CVC or Intermediate CVC of a valid PIV Card[9] shall not be expired.

Note that the option to include an Intermediate CVC is included as a temporary measure to accommodate the use of certification authorities that do not support the issuance of X.509 certificates that contain elliptic curve subject public keys. It is expected that the Intermediate CVC data element will be deprecated in a future version of SP 800-73.

3.3.8 Pairing Code Reference Data Container

The Pairing Code Reference Data Container, which shall be present if the PIV Card supports the virtual contact interface, includes a copy of the PIV Card's pairing code (see Section 5.1.3).

3.4 Inclusion of Universally Unique IDentifiers (UUIDs)

This specification provides support for two UUIDs on a PIV Card. The Card UUID is a UUID that is unique for each card, and it shall be present on all PIV Cards. The Cardholder UUID is a UUID that is a persistent identifier for the cardholder, and it is optional to implement. The requirements for these UUIDs are provided in the following subsections.

3.4.1 Card UUID

FIPS 201 requires PIV Cards to include a Card UUID. The Card UUID shall be included on PIV Cards as follows:

1. The value of the GUID data element of the CHUID data object shall be a 16-byte binary representation of a valid UUID [RFC4122]. The UUID should be version 1, 4, or 5, as specified in [RFC4122, Section 4.1.3].

2. The same 16-byte binary representation of the UUID value shall be present as the value of an entryUUID attribute, as defined in [RFC4530], in any CMS-signed data object that is required to contain a pivFASC-N attribute on a PIV Card, i.e., in the mandatory cardholder fingerprint template and facial image data objects as well as in the optional cardholder iris images data object when present.

3. If the PIV Card supports secure messaging, then the same 16-byte binary representation of the UUID value shall be used as the Subject Identifier in the secure messaging CVC, as specified in Part 2, Section 4.1.5.

4. The string representation of the same UUID value shall be present in the X.509 Certificate for PIV Authentication and the X.509 Certificate for Card Authentication, in the subjectAltName extension encoded as a URI, as specified by [RFC4122, Section 3].

3.4.2 Cardholder UUID

As defined in Section 3.1.2, the CHUID may optionally include a Cardholder UUID. When present, the Cardholder UUID shall be a 16-byte binary representation of a valid UUID, and it shall be version 1, 4, or 5, as specified in [RFC4122, Section 4.1.3].

Deleted: card verifiable certificate

Deleted: (

Deleted:)

[9] A valid PIV Card is defined as a PIV Card that is neither expired nor revoked.

3.5 Data Object Containers and associated Access Rules and Interface Modes

Table 2 defines a high level view of the data model. Each on-card storage container is labeled either as Mandatory (M), Optional (O), or Conditional (C). The conditional data objects are digital signature key and key management key, which are mandatory if the cardholder has a government-issued email account at the time of credential issuance. This data model is designed to enable and support dual interface cards. For dual chip implementations, for any container that can be accessed over both the contact interface and the contactless interface (including the virtual contact interface) the data object shall be copied into the corresponding containers on both chips.[10] Note that access conditions based on the interface mode (contact vs. contactless) take precedence over all Access Rules defined in Table 2, Column 3.

Table 2. Data Model Containers

Container Name	Container ID	Access Rule for Read	Contact / Contactless[11]	M/O/C
Card Capability Container	0xDB00	Always	Contact	M
Card Holder 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	M
X.509 Certificate for Card Authentication	0x0500	Always	Contact and Contactless	M
X.509 Certificate for Digital Signature	0x0100	Always	Contact	C
X.509 Certificate for Key Management	0x0102	Always	Contact	C
Printed Information	0x3001	PIN or OCC	Contact	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
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

[10] As a consequence of this requirement, any keys that have to be generated on card cannot be made available over the contactless interface (including the virtual contact interface) in a dual chip implementation.

[11] Contact interface mode means the container is accessible through contact and virtual contact interfaces only. Contact and contactless interface mode means the container can be accessed from any interface. The term *virtual contact interface* is used in this document as a shorthand for a security condition in which secure messaging is used **AND** the security status indicator associated with the pairing code is TRUE.

Container Name	Container ID	Access Rule for Read	Contact / Contactless[11]	M/O/C
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
Biometric Information Templates Group Template	0x1016	Always	Contact and Contactless	O
Secure Messaging Certificate Signer	0x1017	Always	Contact and Contactless	O
Pairing Code Reference Data Container	0x1018	PIN or OCC	Contact	O

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 in accordance with SP 800-73-4 naming conventions.

4. 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 is 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* (OID), as defined in ISO/IEC 8824-2:2002 [ISO8824].

A data object whose data content is encoded as a BER-TLV data structure as in ISO/IEC 8825-1:2002 [ISO8825] is called a *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 the 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 data objects are BER-TLV objects encoded as per [ISO8825], except that tag values of the PIV data object's inner tag assignments do not conform to BER-TLV requirements.[12] This is due to the need to accommodate legacy tags inherited from [GSC-IS].

Before the card is issued, data objects that are created but not used shall be set to zero-length value.

Deleted: When a data object is created and not personalized, the data object

4.2 OIDs and Tags of PIV Card Application Data Objects

Table 3 lists the ASN.1 object identifiers and BER-TLV tags of the thirty-six PIV Card Application data objects. For the purpose of constructing PIV Card Application data object names in the CardApplicationURL in the 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'.

Deleted: three

4.3 Object Identifiers

Each of the data objects in the PIV Card Application has been provided with a BER-TLV tag and an ASN.1 OID from the NIST personal identity verification arc. These object identifier assignments are given in Table 3.

Deleted: three-byte

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."

[12] The exception does not apply to the BIT Group template, the Discovery Object or the Application Property Template (APT), since these objects use interindustry tags from ISO/IEC 7816-6.

Deleted: to

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 2 lists the ACRs of the thirty-six PIV Card Application data objects. See Table 4 in Section 5.1 and Table 6-3 in Special Publication 800-78 [SP800-78] for the key references and permitted algorithms associated with these authenticable entities.

Deleted: three

Table 3. Object Identifiers of the PIV Data Objects for Interoperable Use

Data Object for Interoperable Use	ASN.1 OID	BER-TLV Tag	M/O/C
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
Cardholder Fingerprints	2.16.840.1.101.3.7.2.96.16	'5FC103'	M
Security Object	2.16.840.1.101.3.7.2.144.0	'5FC106'	M
Cardholder Facial Image	2.16.840.1.101.3.7.2.96.48	'5FC108'	M
X.509 Certificate for Card Authentication	2.16.840.1.101.3.7.2.5.0	'5FC101'	M
X.509 Certificate for Digital Signature	2.16.840.1.101.3.7.2.1.0	'5FC10A'	C
X.509 Certificate for Key Management	2.16.840.1.101.3.7.2.1.2	'5FC10B'	C
Printed Information	2.16.840.1.101.3.7.2.48.1	'5FC109'	O
Discovery Object	2.16.840.1.101.3.7.2.96.80	'7E'	O
Key History Object	2.16.840.1.101.3.7.2.96.96	'5FC10C'	O
Retired X.509 Certificate for Key Management 1	2.16.840.1.101.3.7.2.16.1	'5FC10D'	O
Retired X.509 Certificate for Key Management 2	2.16.840.1.101.3.7.2.16.2	'5FC10E'	O
Retired X.509 Certificate for Key Management 3	2.16.840.1.101.3.7.2.16.3	'5FC10F'	O
Retired X.509 Certificate for Key Management 4	2.16.840.1.101.3.7.2.16.4	'5FC110'	O
Retired X.509 Certificate for Key Management 5	2.16.840.1.101.3.7.2.16.5	'5FC111'	O
Retired X.509 Certificate for Key Management 6	2.16.840.1.101.3.7.2.16.6	'5FC112'	O
Retired X.509 Certificate for Key Management 7	2.16.840.1.101.3.7.2.16.7	'5FC113'	O
Retired X.509 Certificate for Key Management 8	2.16.840.1.101.3.7.2.16.8	'5FC114'	O
Retired X.509 Certificate for Key Management 9	2.16.840.1.101.3.7.2.16.9	'5FC115'	O
Retired X.509 Certificate for Key Management 10	2.16.840.1.101.3.7.2.16.10	'5FC116'	O
Retired X.509 Certificate for Key Management 11	2.16.840.1.101.3.7.2.16.11	'5FC117'	O
Retired X.509 Certificate for Key Management 12	2.16.840.1.101.3.7.2.16.12	'5FC118'	O
Retired X.509 Certificate for Key Management 13	2.16.840.1.101.3.7.2.16.13	'5FC119'	O
Retired X.509 Certificate for Key Management 14	2.16.840.1.101.3.7.2.16.14	'5FC11A'	O
Retired X.509 Certificate for Key Management 15	2.16.840.1.101.3.7.2.16.15	'5FC11B'	O
Retired X.509 Certificate for Key Management 16	2.16.840.1.101.3.7.2.16.16	'5FC11C'	O
Retired X.509 Certificate for Key Management 17	2.16.840.1.101.3.7.2.16.17	'5FC11D'	O
Retired X.509 Certificate for Key Management 18	2.16.840.1.101.3.7.2.16.18	'5FC11E'	O
Retired X.509 Certificate for Key Management 19	2.16.840.1.101.3.7.2.16.19	'5FC11F'	O
Retired X.509 Certificate for Key Management 20	2.16.840.1.101.3.7.2.16.20	'5FC120'	O
Cardholder Iris Images	2.16.840.1.101.3.7.2.16.21	'5FC121'	O
Biometric Information Templates Group Template	2.16.840.1.101.3.7.2.16.22	'7F61'	O
Secure Messaging Certificate Signer	2.16.840.1.101.3.7.2.16.23	'5FC122'	O
Pairing Code Reference Data Container	2.16.840.1.101.3.7.2.16.24	'5FC123'	O

5. Data Types and Their Representation

This section provides a description of the data types used in the PIV Client Application Programming Interface (SP 800-73-4, Part 3) and PIV Card Command Interface (SP 800-73-4, 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 smart card 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.[13]

5.1 Key References

A key reference is a one-byte reference data identifier that specifies a cryptographic key or PIN according to its PIV Key Type. Table 4 and SP 800-78, Table 6-1, define the key reference values that shall be used on the PIV interfaces. The key reference values are used, for example, in a cryptographic protocol such as an authentication or a signing protocol. Key references are only assigned to private and secret (symmetric) keys, PINs, PIN Unblocking Key (PUK), OCC, and the pairing code. All other PIV Card Application key reference values are reserved for future use.

Table 4. PIV Card Application Authentication and Key References

Key Reference Value	PIV Reference Data Type	Authenticable Entity	Security Condition for Use		Retry Reset Value	Number of Unblocks
			Contact	Contactless		
'00'	Global PIN	Cardholder	Always	VCI	Platform Specific	Platform Specific
'80'	PIV Card Application PIN	Cardholder	Always	VCI	Issuer Specific	Issuer Specific
'81'	PIN Unblocking Key	PIV Card Application Administrator	Always	Never	Issuer Specific	Issuer Specific
'96'	Primary Finger OCC	Cardholder	Always	SM	Issuer Specific	Issuer Specific
'97'	Secondary Finger OCC	Cardholder	Always	SM	Issuer Specific	Issuer Specific
'98'	Pairing Code	Cardholder	Always[14]	SM	Issuer Specific	Issuer Specific

Deleted: Key

Deleted: / *Administrator*

[13] A customized Part 1 data model exists in the PIV-Interoperable card (PIV-I card) specification as defined in [PIV-I NFI] and further clarified in [PIV-I FAQ]. The intent of [PIV-I NFI] is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and their applications, and that may be trusted for particular purposes at the discretion of the relying Federal departments and agencies. PIV-I cards use the same namespace and data types as PIV Cards, however, the data model is slightly different since some of the ASN.1 OIDs that appear in PIV certificates are specific to PIV Cards and since non-Federal issuers do not have Agency Codes assigned to them, which means that they are unable to create unique FASC-N identifiers for the cards they issue. As a result, [PIV-I FAQ] requires the first 14 digits of the FASC-Ns for PIV-I cards (the Agency Code, System Code, and Credential Number) to be populated with all nines.

[14] The sole use of the pairing code is the establishment of a VCI. Its use over the contact interface serves no purpose.

Key Reference Value	PIV Key Type	Administrator	Security Condition for Use	
			Contact	Contactless
'03'	PIV Secure Messaging Key	PIV Card Application Administrator	Always	Always
'9A'	PIV Authentication Key	PIV Card Application Administrator	PIN or OCC	VCI and (PIN or OCC)
'9B'	PIV Card Application Administration Key	PIV Card Application Administrator	Always	Never
'9C'	Digital Signature Key	PIV Card Application Administrator	PIN Always or OCC Always	VCI and (PIN Always or OCC Always)
'9D'	Key Management Key	PIV Card Application Administrator	PIN or OCC	VCI and (PIN or OCC)
'9E'	Card Authentication Key[15]	PIV Card Application Administrator	Always	Always
'82', '83', '84', '85', '86', '87', '88', '89', '8A', '8B', '8C', '8D', '8E', '8F', '90', '91', '92', '93', '94', '95'	Retired Key Management Key	PIV Card Application Administrator	PIN or OCC	VCI and (PIN or OCC)

Deleted: Authenticable Entity /

Secure Messaging (SM) is defined in Section 5.4 and VCI is defined in Section 5.5. Table 2 of Part 2 specifies the security conditions for each command.

When represented as a byte, the key reference occupies bits 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 cardholder Global PIN or OCC data. If the Global PIN is used by the PIV Card Application then the Global PIN format shall follow the PIV Card Application PIN format defined in Section 2.4.3 of Part 2.

PIV Card Applications with the Discovery Object, and the first byte of the PIN Usage Policy value set to 0x60, 0x68, 0x70, or 0x78 as per Section 3.3.2, shall reference the PIV Card Application PIN as well as the cardholder Global PIN in the access control rules for PIV data object access.

Deleted: 0

[15] A card may optionally have a symmetric CAK in addition to the mandatory asymmetric CAK, in which case both keys would share the same key reference and access control rules.

Additionally, the PIV Card Application card commands can change the status of the Global PIN, and may change its reference data while the PIV Card Application is the currently selected application.

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

5.1.1 OCC Data

This document does not specify how the biometric reference data and comparison parameters are stored internally on the card. Moreover, the export of the biometric reference data shall not be allowed. Configuration data related to the biometric reference data may be read from the tag 0x7F61 BIT Group Template data object (see Section 3.3.6). Configuration data is defined in Table 7 of [SP800-76].

Deleted: tag 0x7F61

Deleted: as described in Section 3.3.

Deleted: 2

5.1.2 PIV Secure Messaging Key

If the PIV Card supports secure messaging, the PIV Secure Messaging key shall be generated on the PIV Card and the PIV Card shall not permit exportation of the PIV Secure Messaging key. The cryptographic operations that use the PIV Secure Messaging key shall be available through the contact and contactless interfaces of the PIV Card. The PKI cryptographic function (see Table 4) is under an "Always" access rule, and thus private key operations (i.e., use of the key to establish session keys for secure messaging) can be performed without access control restrictions.

Deleted: protected with

Deleted: . In other words,

Deleted: may

The PIV Card shall store a corresponding secure messaging CVC to support validation of the public key by the relying party. The format for the secure messaging CVC shall be as specified in Part 2, Section 4.1.5. The public key required to verify the digital signature of the secure messaging CVC shall be provided in a certificate in the Secure Messaging Certificate Signer data object, as specified in Section 3.3.7.

Deleted: card verifiable certificate (

Deleted:)

Deleted: content signing certificate, which shall be an X.509 digital signature certificate issued under the id-fpki-common-piv-contentSigning policy of [COMMON]. The content signing certificate shall also include an extended key usage (*extKeyUsage)* extension asserting id-PIV-content-signing. The content signing certificate shall be publicly available via a URL specified in the Discovery Object (see Section 3.3.2). Additional descriptions for the PIV object identifiers are provided in Appendix B of FIPS 201-2. The content signing certificate needed to verify the digital signature of a CVC of a valid PIV Card

Deleted: [16] shall not be expired

5.1.3 Pairing Code

If the PIV Card supports the virtual contact interface then it shall implement support for the pairing code. If implemented, the pairing code shall consist of eight decimal digits and it shall be generated at random by the PIV Card Issuer. The results of each random pairing code generation shall be loaded onto at most one PIV Card and cannot be changed by the cardholder. The pairing code value for a PIV Card shall be stored in the Pairing Code Reference Data Container (see Section 3.3.8) on the card and may be printed on the back of the card in an agency-specific text area (Zones 9B or 10B). PIV Card Issuers may choose to provide the pairing code value to the cardholder in another manner, such as printing it on a slip of paper, rather than printing it on the back of the card.[17]

Unlike the PIV Card Application PIN or the Global PIN, there are no restrictions on the caching of the pairing code by client applications. It is recommended that a client application that needs to communicate with a PIV Card over its virtual contact interface obtain the card's pairing code during a registration step, either by asking the cardholder to enter the value or by reading it from the card over the contact interface from the Pairing Code Reference Data Container, and then cache the pairing

[17] While printing the value of the pairing code on the back of the card provides maximum convenience for use by the cardholder and avoids any risk that the cardholder will forget the pairing code, it may create a risk that an attacker could obtain the value of the pairing code by surreptitiously reading it from the back of the card. Departments and agencies will need to make a risk-based decision in determining the method by which they provide cardholders with the values of their pairing codes.

code until the card expires. The client application may then connect to the card and establish a virtual contact interface with it whenever the card is within read-range of the client application's contactless card reader without needing to prompt the cardholder.

5.2 PIV Algorithm Identifier

A PIV algorithm identifier is 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., 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 5. These identifiers serve as inputs to the GENERATE ASYMMETRIC KEY PAIR card command and the Part 3 pivGenerateKeyPair() client API function call, which initiates the generation and storage of the asymmetric key pair.

Table 5. Cryptographic Mechanism Identifiers

Cryptographic Mechanism Identifier	Description	Parameter
'07'	RSA 2048	Optional public exponent encoded big-endian
'11'	ECC: Curve P-256	None
'14'	ECC: Curve P-384	None

Deleted: '06' ...

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

5.4 Secure Messaging

A PIV Card Application may optionally support secure messaging (SM). When secure messaging is established, the PIV Card Application is authenticated to the relying system and a set of symmetric session keys are established, which are used to provide confidentiality and integrity protection for the card commands that are sent to the card using secure messaging as well as for the responses from the PIV Card.

Deleted: S

Deleted: M

If implemented, SM for non-card-management operations shall only be established using the PIV Secure Messaging key specified in Table 4 and the SM protocol in accordance with the specifications in Section 4 of Part 2.

5.5 Virtual Contact Interface

Once secure messaging has been established over the contactless interface, a VCI may be established by the presentation of the pairing code to the PIV Card using secure messaging. Any command sent to the card using secure messaging while the security status indicator associated with the pairing code is TRUE is considered to be sent over the VCI. All non-card-management operations that are allowed over contact interface may be carried out over the VCI. Support for the VCI is optional.

Deleted: a valid

Deleted: and the pairing code

5.6 Status Words

A Status Word (SW) is a 2-byte value returned by 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 the card command interface and their interpretation are given in Table 6. The descriptions of individual card commands provide additional information for interpreting returned status words.

Table 6. Status Words

SW1	SW2	Meaning
'61'	'xx'	Successful execution where SW2 encodes the number of response data bytes still available
'63'	'00'	Verification failed
'63'	'CX'	Verification failed, X indicates the number of further allowed retries or resets
'68'	'82'	Secure messaging not supported
'69'	'82'	Security status not satisfied
'69'	'83'	Authentication method blocked
'69'	'87'	Expected secure messaging data objects are missing
'69'	'88'	Secure messaging data objects are incorrect
'6A'	'80'	Incorrect parameter in command data field
'6A'	'81'	Function not supported
'6A'	'82'	Data object or application not found
'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 SP 800-73-4 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. For each container, compliant cards shall return all TLV elements of the container in the order listed in this appendix.

Both single-chip/dual-interface and dual-chip implementations are 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 7. PIV Data Containers

Container Description	ContainerID	BER-TLV Tag	Container Minimum Capacity (Bytes)[18]	Access Rule for Read	Contact / Contactless[19]	M/O/C
Card Capability Container	0xDB00	'5FC107'	297	Always	Contact	M
Card Holder Unique Identifier	0x3000	'5FC102'	2916	Always	Contact and Contactless	M
X.509 Certificate for PIV Authentication (Key Reference '9A')	0x0101	'5FC105'	2005	Always	Contact	M
Cardholder Fingerprints	0x6010	'5FC103'	4006	PIN	Contact	M
Security Object	0x9000	'5FC106'	1337	Always	Contact	M
Cardholder Facial Image	0x6030	'5FC108'	12710	PIN	Contact	M
X.509 Certificate for Card Authentication (Key Reference '9E')	0x0500	'5FC101'	2005	Always	Contact and Contactless	M
X.509 Certificate for Digital Signature (Key Reference '9C')	0x0100	'5FC10A'	2005	Always	Contact	C
X.509 Certificate for Key Management (Key Reference '9D')	0x0102	'5FC10B'	2005	Always	Contact	C
Printed Information	0x3001	'5FC109'	190	PIN or OCC	Contact	O
Discovery Object	0x6050	'7E'	20	Always	Contact and Contactless	O
Key History Object	0x6060	'5FC10C'	128	Always	Contact	O

Deleted: 2

Deleted: 9

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

[19] Contact interface mode means the container is accessible through contact and virtual contact interfaces only. Contact and contactless interface mode means the container can be accessed from any interface.

Container Description	ContainerID	BER-TLV Tag	Container Minimum Capacity (Bytes)[18]	Access Rule for Read	Contact / Contactless[19]	M/O/C
Retired X.509 Certificate for Key Management 1 (Key reference '82')	0x1001	'5FC10D'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 2 (Key reference '83')	0x1002	'5FC10E'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 3 (Key reference '84')	0x1003	'5FC10F'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 4 (Key reference '85')	0x1004	'5FC110'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 5 (Key reference '86')	0x1005	'5FC111'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 6 (Key reference '87')	0x1006	'5FC112'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 7(Key reference '88')	0x1007	'5FC113'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 8(Key reference '89')	0x1008	'5FC114'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 9 (Key reference '8A')	0x1009	'5FC115'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 10 (Key reference '8B')	0x100A	'5FC116'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 11 (Key reference '8C')	0x100B	'5FC117'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 12 (Key reference '8D')	0x100C	'5FC118'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 13 (Key reference '8E')	0x100D	'5FC119'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 14 (Key reference '8F')	0x100E	'5FC11A'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 15 (Key reference '90')	0x100F	'5FC11B'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 16 (Key reference '91')	0x1010	'5FC11C'	2005	Always	Contact	O

Container Description	ContainerID	BER-TLV Tag	Container Minimum Capacity (Bytes)[18]	Access Rule for Read	Contact / Contactless[19]	M/O/C
Retired X.509 Certificate for Key Management 17 (Key reference '92')	0x1011	'5FC11D'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 18 (Key reference '93')	0x1012	'5FC11E'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 19 (Key reference '94')	0x1013	'5FC11F'	2005	Always	Contact	O
Retired X.509 Certificate for Key Management 20 (Key reference '95')	0x1014	'5FC120'	2005	Always	Contact	O
Cardholder Iris Images	0x1015	'5FC121'	7106	PIN	Contact	O
Biometric Information Templates Group Template	0x1016	'7F61'	65	Always	Contact and Contactless	O
Secure Messaging Certificate Signer	0x1017	'5FC122'	2471	Always	Contact and Contactless	O
Pairing Code Reference Data Container	0x1018	'5FC123'	12	PIN or OCC	Contact	O

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

Table 8. Card Capability Container

Card Capability Container		0xDB00	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes[*]**
Card Identifier	0xF0	Fixed	0 or 21
Capability Container version number	0xF1	Fixed	0 or 1
Capability Grammar version number	0xF2	Fixed	0 or 1
Applications CardURL	0xF3	Variable	128
PKCS#15	0xF4	Fixed	0 or 1
Registered Data Model number	0xF5	Fixed	1
Access Control Rule Table	0xF6	Fixed	0 or 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

Note: The optional Extended Application CardURL and Security Object Buffer data elements are deprecated and will be eliminated in a future version of SP 800-73.

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

Table 9. 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	25
Organizational Identifier (Optional)	0x32	Fixed	4
DUNS (Optional)	0x33	Fixed	9
GUID	0x34	Fixed	16
Expiration Date	0x35	Date (YYYYMMDD)	8
Cardholder UUID (Optional)	0x36	Fixed	16
Issuer Asymmetric Signature	0x3E	Variable	2816[**]
Error Detection Code	0xFE	LRC	0

Deleted: Unique Identification Number

Note: The optional Buffer Length, Organizational Identifier and DUNS data elements are deprecated and will be eliminated in a future version of SP 800-73.

The Error Detection Code is the same element as the Longitudinal Redundancy Code (LRC) in [TIG SCEPACS]. Because TIG SCEPACS makes the LRC mandatory, it is present in the CHUID. However, this document makes no use of the Error Detection Code, and therefore the length of the TLV value is set to 0 bytes (i.e., no value will be supplied).

Table 10. 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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 11. Cardholder Fingerprints

Cardholder Fingerprints		0x6010	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes[*]**
Fingerprint I & II	0xBC	Variable	4000[****]
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: The signer certificate may cause the "Max. Bytes" value in the Issuer Asymmetric Signature field to be exceeded.

[***] Recommended length. Certificate size can exceed indicated length value.

[****] Recommended length. The certificate that signed the Fingerprint I & II data element in the Cardholder Fingerprints data object can either be stored in the CHUID or in the Fingerprint I & II data element itself. If the latter, the "Max. Bytes" value quoted is a recommendation and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the "Max. bytes."

Table 12. Security Object

Security Object		0x9000	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes[*]**
Mapping of DG to ContainerID	0xBA	Variable	30
Security Object	0xBB	Variable	1298
Error Detection Code	0xFE	LRC	0

Deleted: 10

Deleted: 20

Table 13. Cardholder Facial Image

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

Table 14. Printed Information

Printed Information		0x3001	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes[*]**
Name	0x01	Text (ASCII)	125
Employee Affiliation	0x02	Text (ASCII)	20
Expiration date	0x04	Date (YYYYMMMDD)	9
Agency Card Serial Number	0x05	Text (ASCII)	20
Issuer Identification	0x06	Fixed Text (ASCII)	15
Organization Affiliation (Line 1) (Optional)	0x07	Text (ASCII)	20
Organization Affiliation (Line 2) (Optional)	0x08	Text (ASCII)	20
Error Detection Code	0xFE	LRC	0

In order to successfully match the printed information for verification on Zone 8F (Employee Affiliation) and Zone 10F (Agency, Department, or Organization) on the face of the card with the printed information stored electronically on the card, agencies should use tags 0x02, 0x07 and 0x08.

Table 15. X.509 Certificate for Digital Signature

X.509 Certificate for Digital Signature		0x0100	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

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

[*****] Recommended length. The certificate that signed the Image for Visual Verification data element (tag 0xBC) can be stored in the CHUID or in the Image for Visual Verification data element itself. If the latter, the "Max. Bytes" value quoted is a recommendation and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the "Max. bytes."

[***] Recommended length. Certificate size can exceed indicated length value.

Table 16. X.509 Certificate for Key Management

X.509 Certificate for Key Management		0x0102	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 17. X.509 Certificate for Card Authentication

X.509 Certificate for Card Authentication		0x0500	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 18. Discovery Object

Discovery Object (Tag '7E')		0x6050	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes[*]**
PIV Card Application AID	0x4F	Fixed	12
PIN Usage Policy	0x5F2F	Fixed	2

Deleted: 3

Deleted: Biometric Information Templates Group Template (Conditional)[20]

Table 19. Key History Object

Key History Object		0x6060	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes[*]**
keysWithOnCardCerts	0xC1	Fixed	1
keysWithOffCardCerts	0xC2	Fixed	1[22]
offCardCertURL (Conditional)[23]	0xF3	Variable	118
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.

[22] The numeric values indicated in keysWithOnCardCerts and keysWithOffCardCerts are represented as unsigned binary integers.

[23] The offCardCertURL data element shall be present if keysWithOffCardCerts is greater than zero and shall be absent if both keysWithOnCardCerts and keysWithOffCardCerts are zero. The offCardCertURL may be present if keyWithOffCardCerts is zero but keysWithOnCardCerts is greater than zero.

Table 20. Retired X.509 Certificate for Key Management 1

Retired X.509 Certificate for Key Management 1		0x1001	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 21. Retired X.509 Certificate for Key Management 2

Retired X.509 Certificate for Key Management 2		0x1002	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 22. Retired X.509 Certificate for Key Management 3

Retired X.509 Certificate for Key Management 3		0x1003	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 23. Retired X.509 Certificate for Key Management 4

Retired X.509 Certificate for Key Management 4		0x1004	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

[*] 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 24. Retired X.509 Certificate for Key Management 5

Retired X.509 Certificate for Key Management 5		0x1005	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 25. Retired X.509 Certificate for Key Management 6

Retired X.509 Certificate for Key Management 6		0x1006	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 26. Retired X.509 Certificate for Key Management 7

Retired X.509 Certificate for Key Management 7		0x1007	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 27. Retired X.509 Certificate for Key Management 8

Retired X.509 Certificate for Key Management 8		0x1008	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

[*] 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 28. Retired X.509 Certificate for Key Management 9

Retired X.509 Certificate for Key Management 9		0x1009	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 29. Retired X.509 Certificate for Key Management 10

Retired X.509 Certificate for Key Management 10		0x100A	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 30. Retired X.509 Certificate for Key Management 11

Retired X.509 Certificate for Key Management 11		0x100B	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 31. Retired X.509 Certificate for Key Management 12

Retired X.509 Certificate for Key Management 12		0x100C	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

[*] 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 32. Retired X.509 Certificate for Key Management 13

Retired X.509 Certificate for Key Management 13	0x100D		
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 33. Retired X.509 Certificate for Key Management 14

Retired X.509 Certificate for Key Management 14	0x100E		
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 34. Retired X.509 Certificate for Key Management 15

Retired X.509 Certificate for Key Management 15	0x100F		
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 35. Retired X.509 Certificate for Key Management 16

Retired X.509 Certificate for Key Management 16	0x1010		
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

[*] 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 36. Retired X.509 Certificate for Key Management 17

Retired X.509 Certificate for Key Management 17		0x1011	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 37. Retired X.509 Certificate for Key Management 18

Retired X.509 Certificate for Key Management 18		0x1012	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 38. Retired X.509 Certificate for Key Management 19

Retired X.509 Certificate for Key Management 19		0x1013	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

Table 39. Retired X.509 Certificate for Key Management 20

Retired X.509 Certificate for Key Management 20		0x1014	
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

Note: The optional MSCUID data element is deprecated and will be eliminated in a future version of SP 800-73.

The CertInfo byte in the certificate data objects identified in this appendix shall be encoded as follows:

[*] 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.

b8	b7	b6	b5	b4	b3	b2	b1
RFU8	RFU7	RFU6	RFU5	RFU4	IsX509	CompressionTypeLsb	CompressionTypeMsb

CompressionTypeMsb shall be 0 if the certificate is encoded in uncompressed form and 1 if the certificate is encoded using GZIP compression.[24] CompressionTypeLsb and IsX509 shall be set to 0 for PIV Card Applications. Thus, for a certificate encoded in uncompressed form CertInfo shall be 0x00, and for a certificate encoded using GZIP compression CertInfo shall be 0x01.

Table 40. Cardholder Iris Images

Cardholder Iris Images	0x1015		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Images for Iris	0xBC	Variable	7100******
Error Detection Code	0xFE	LRC	0

Table 41. Biometric Information Templates Group Template

BIT Group Template (Tag '7F61')	0x1016		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Number of Fingers	0x02	Fixed	1
BIT for first Finger	0x7F60	Variable	28
BIT for second Finger (Optional)	0x7F60	Variable	28

Table 42. Secure Messaging Certificate Signer

Secure Messaging Certificate Signer	0x1017		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
X.509 Certificate for Content Signing	0x70	Variable	1856
CertInfo	0x71	Fixed	1
Intermediate CVC (Conditional)[25]	0x7F21	Variable	601
Error Detection Code	0xFE	LRC	0

The CertInfo byte in the Secure Messaging Certificate Signer data object shall provide information about the X.509 Certificate for Content Signing. The Intermediate CVC, if present, shall be stored in uncompressed form.

Table 43. Pairing Code Reference Data Container

Pairing Code	0x1018		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes***
Pairing Code	0x99	Fixed Text (ASCII)	8
Error Detection Code	0xFE	LRC	0

[24] GZIP formats are specified in RFC 1951 and RFC 1952.

****** Recommended length. The certificate that signed the Images for Iris data element (tag 0xBC) can be stored in the CHUID or in the Images for Iris data element itself. If the latter, the "Max. Bytes" value quoted is a recommendation and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the "Max. bytes."

[25] The Intermediate CVC shall be absent if the X.509 Certificate for Content Signing contains the public key needed to verify the signature on the secure messaging CVC and shall be present otherwise.

Appendix B––PIV Authentication Mechanisms

To provide guidelines on the usage and behavior supported by the PIV Card, PIV authentication mechanisms 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; and
- 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, 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; and
- 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 to whom the card has been issued. 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 or iris image 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; and

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

B.1 Authentication Mechanism Diagrams

This section describes the activities and interactions involved in interoperable usage and authentication of the PIV Card. The authentication mechanisms 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 authentication mechanism 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 illustrations, the validation steps are marked as CardV, CredV, and HolderV to signify Card, Credential, and Cardholder validation respectively.

Depending on 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 Biometrics (BIO)

The general authentication mechanism using the PIV biometrics is illustrated in Figure B-1.

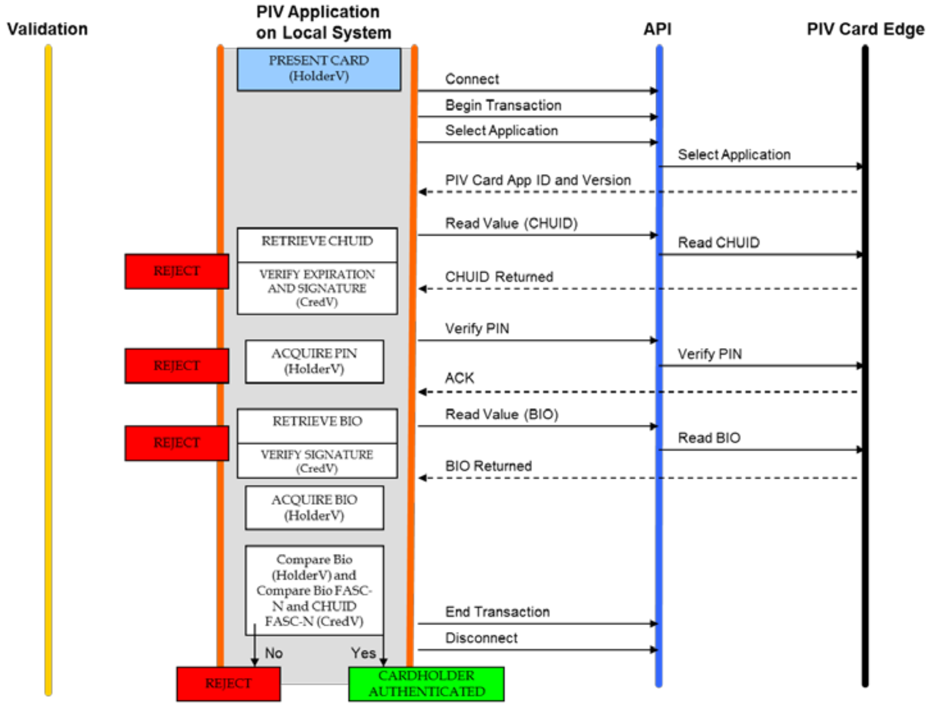

Figure B-1. Authentication using PIV Biometrics (BIO)

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. The attended biometric authentication mechanism (BIO-A) is illustrated in Figure B-2.

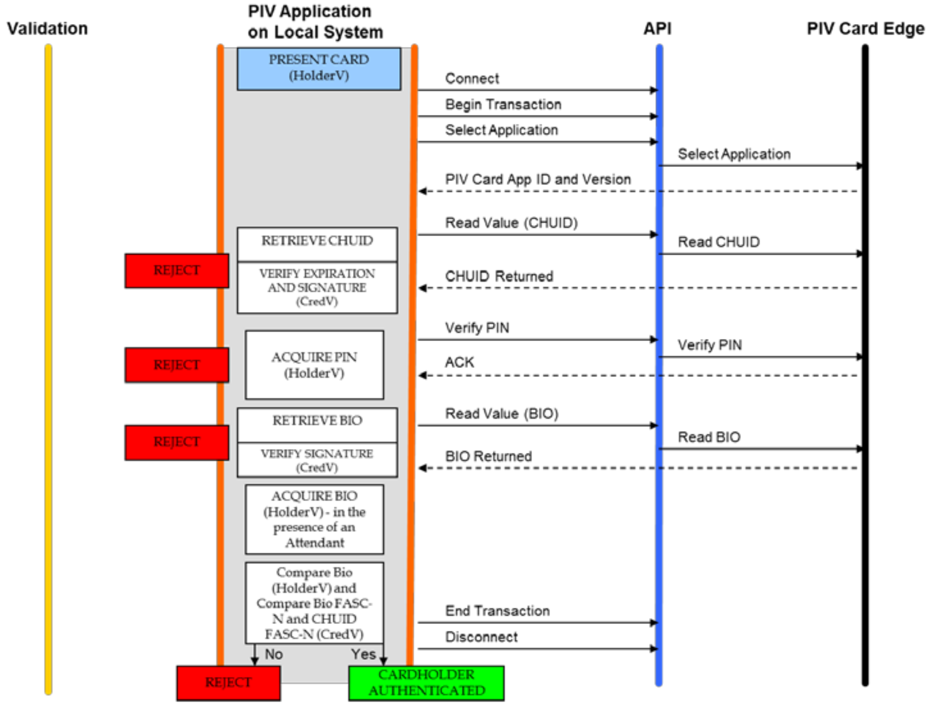

Figure B-2. Authentication using PIV Biometrics Attended (BIO-A)

B.1.2 Authentication Using PIV Authentication Key

The authentication mechanism using the PIV Authentication key is illustrated in Figure B-3.

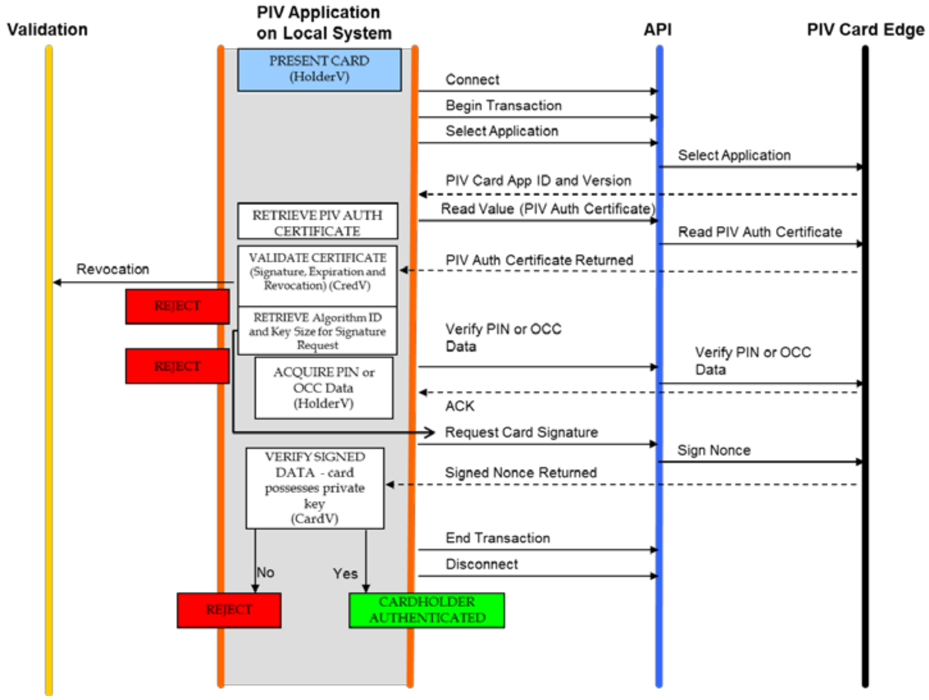
Validation
PIV Application on Local System
API
PIV Card Edge
PRESENT CARD (HolderV)
Connect
Begin Transaction
Select Application
Select Application
PIV Card App ID and Version
RETRIEVE PIV AUTH CERTIFICATE
Read Value (PIV Auth Certificate)
Read PIV Auth Certificate
VALIDATE CERTIFICATE (Signature, Expiration and Revocation) (CredV)
PIV Auth Certificate Returned
Revocation
REJECT
RETRIEVE Algorithm ID and Key Size for Signature Request
REJECT
Verify PIN or OCC Data
Verify PIN or OCC Data
ACQUIRE PIN or OCC Data (HolderV)
ACK
Request Card Signature
Sign Nonce
VERIFY SIGNED DATA - card possesses private key (CardV)
Signed Nonce Returned
End Transaction
Disconnect
No
Yes
REJECT
CARDHOLDER AUTHENTICATED

Figure B-3. Authentication using PIV Authentication Key

B.1.3 Authentication Using Card Authentication Key

Authentication mechanisms using the Card Authentication key are illustrated in Figures B-4 and B-5. Figure B-4 illustrates the use of the mandatory asymmetric Card Authentication key, while Figure B-5 uses the optional symmetric Card Authentication key for the authentication mechanism.

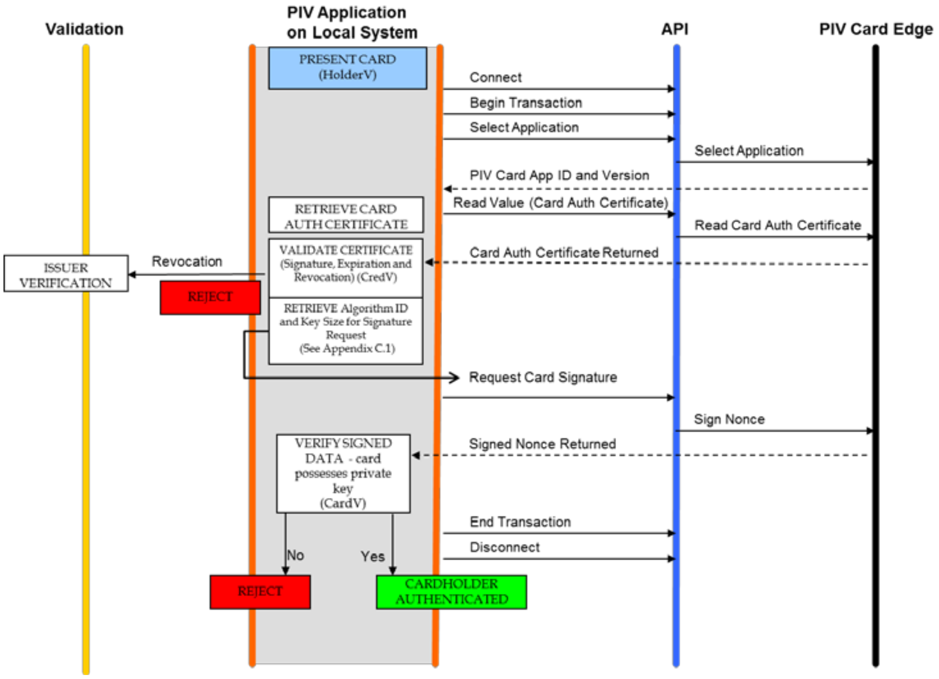
Validation
PIV Application on Local System
API
PIV Card Edge
PRESENT CARD (HolderV)
Connect
Begin Transaction
Select Application
Select Application
PIV Card App ID and Version
Read Value (Card Auth Certificate)
RETRIEVE CARD AUTH CERTIFICATE
Read Card Auth Certificate
ISSUER VERIFICATION
Revocation
VALIDATE CERTIFICATE (Signature, Expiration and Revocation) (CredV)
Card Auth Certificate Returned
REJECT
RETRIEVE Algorithm ID and Key Size for Signature Request (See Appendix C.1)
Request Card Signature
Sign Nonce
VERIFY SIGNED DATA - card possesses private key (CardV)
Signed Nonce Returned
End Transaction
Disconnect
No
Yes
REJECT
CARDHOLDER AUTHENTICATED

Figure B-4. Authentication using an asymmetric Card Authentication Key

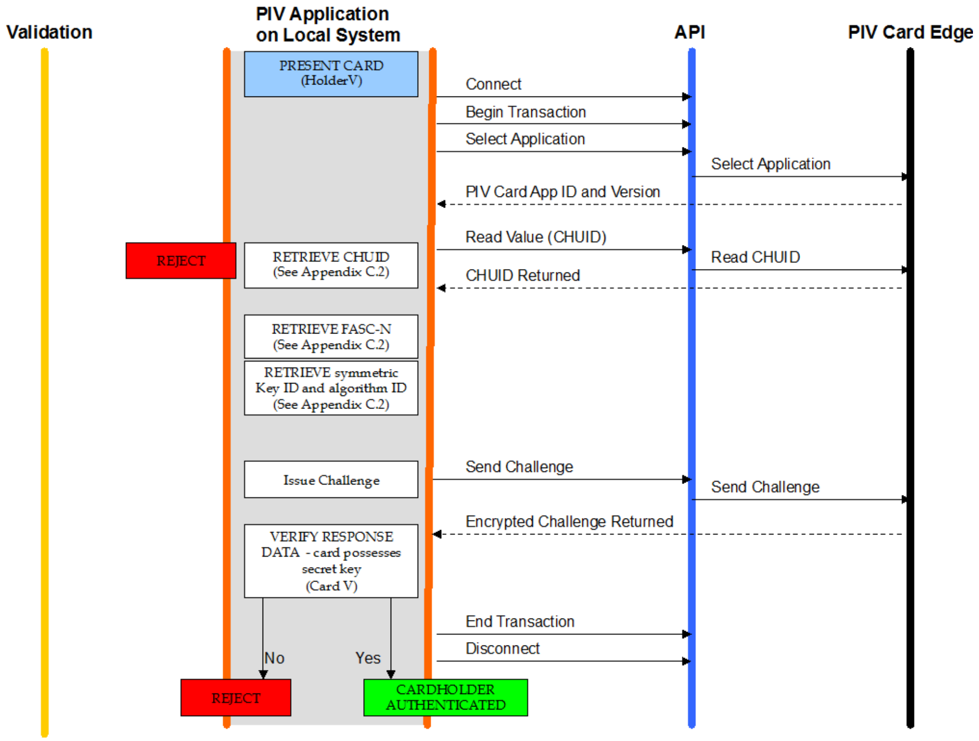
Validation
PIV Application on Local System
API
PIV Card Edge
PRESENT CARD (HolderV)
Connect
Begin Transaction
Select Application
Select Application
PIV Card App ID and Version
REJECT
RETRIEVE CHUID (See Appendix C.2)
Read Value (CHUID)
Read CHUID
CHUID Returned
RETRIEVE FASC-N (See Appendix C.2)
RETRIEVE symmetric Key ID and algorithm ID (See Appendix C.2)
Issue Challenge
Send Challenge
Send Challenge
Encrypted Challenge Returned
VERIFY RESPONSE DATA - card possesses secret key (Card V)
End Transaction
Disconnect
No
Yes
REJECT
CARDHOLDER AUTHENTICATED

Figure B-5. Authentication using a symmetric Card Authentication Key

B.1.4 Authentication Using OCC (OCC-AUTH)

The OCC-AUTH authentication mechanism is implemented by performing on-card biometric comparison (OCC) over secure messaging. The PIV Application authenticates the PIV Card as part of the process of establishing secure messaging. When the live-scan biometric is supplied to the card for OCC over secure messaging, both the request and the response are protected using message authentication codes (MAC), allowing the PIV Application on the local system to verify that the response has not been altered and that it was created by the PIV Card that was authenticated during the establishment of secure messaging.

The OCC-AUTH authentication mechanism is performed by establishing secure messaging as described in Section 4 of Part 2 and then performing the VERIFY command, as illustrated in Figure B-6.

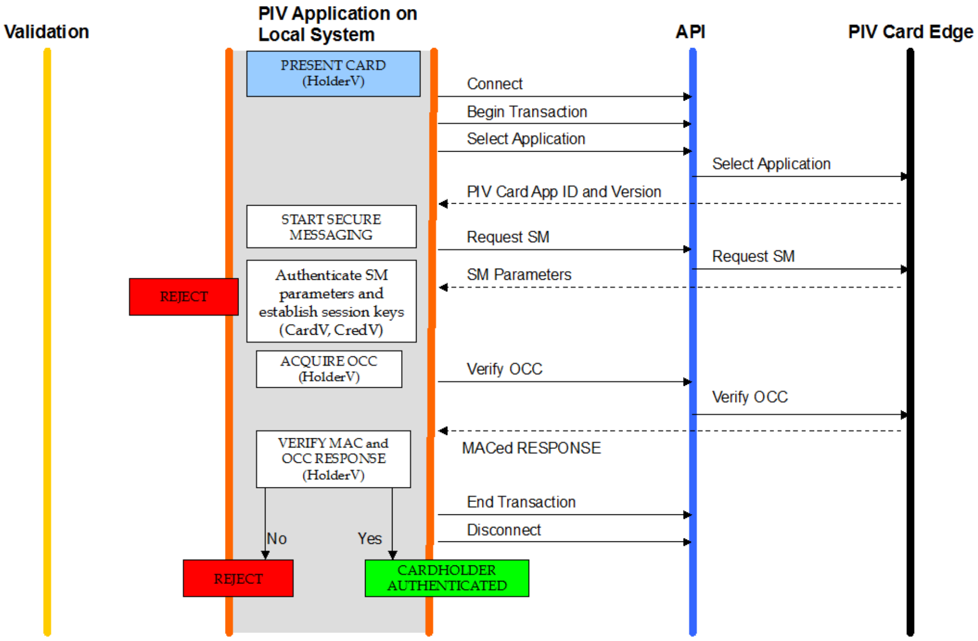

Figure B-6. Authentication using OCC

B.1.5 Authentication Using PIV Visual Credentials

This is the authentication mechanism where a human guard authenticates the cardholder using the visual credentials held by the PIV Card, and is illustrated in Figure B-7.

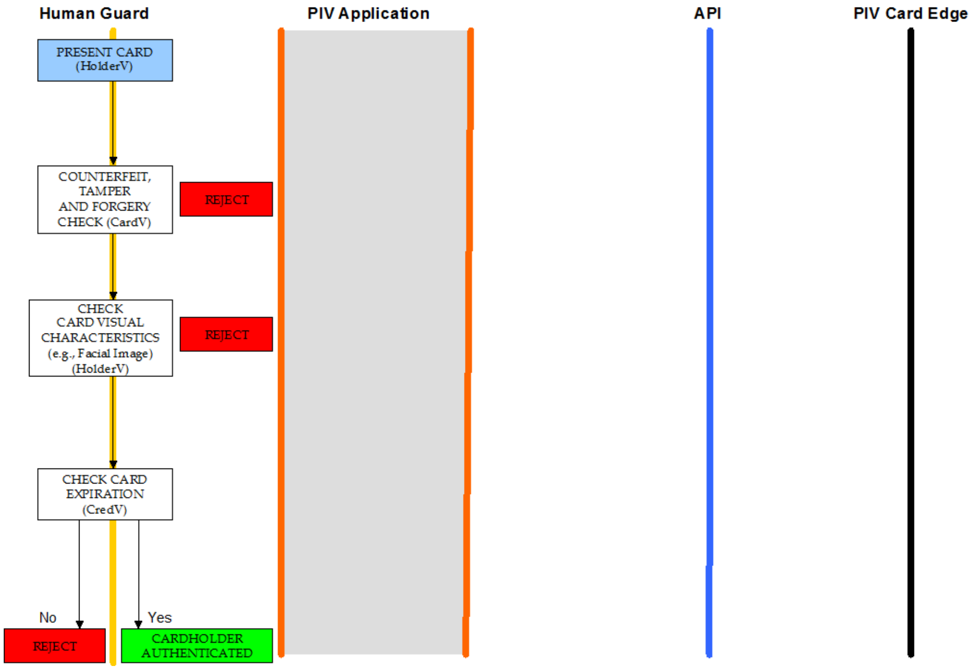
Human Guard
PIV Application
API
PIV Card Edge
PRESENT CARD (HolderV)
COUNTERFEIT, TAMPER AND FORGERY CHECK (CardV)
REJECT
CHECK CARD VISUAL CHARACTERISTICS (e.g., Facial Image) (HolderV)
REJECT
CHECK CARD EXPIRATION (CredV)
No
Yes
REJECT
CARDHOLDER AUTHENTICATED

Figure B-7. Authentication using PIV Visual Credentials

B.1.6 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 authentication mechanism is illustrated in Figure B-8. 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.

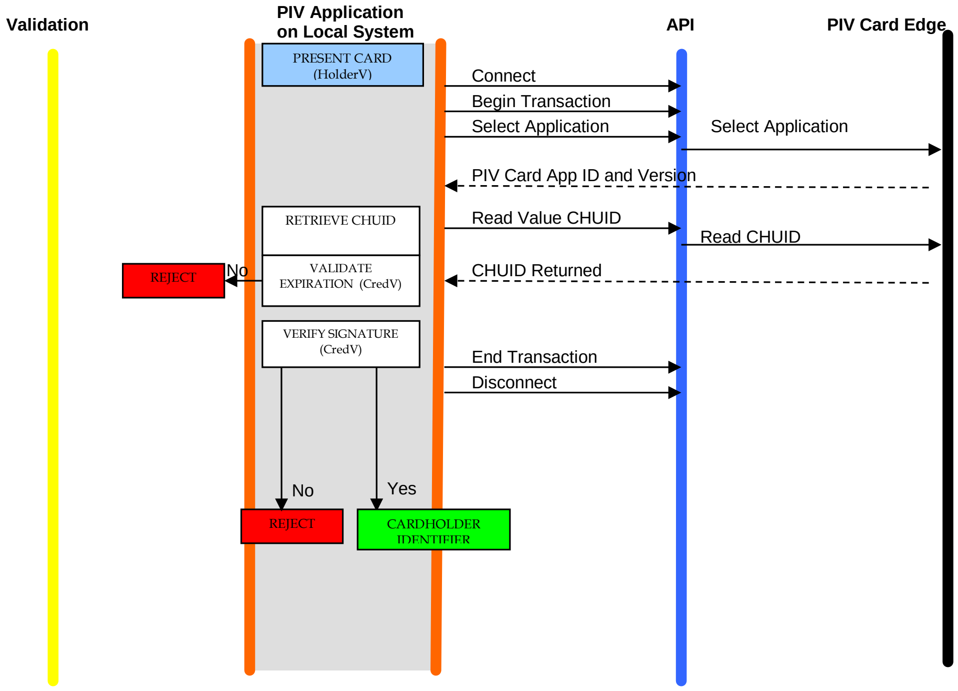

Figure B-8. Authentication using PIV CHUID

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 44 Summary of PIV Authentication Mechanisms

Deleted: 1

PIV Authentication Mechanism	Card Validation Steps (CardV)	Credential Validation Steps (CredV)	Cardholder Validation Steps (HolderV)
PIV Biometric		Expiration check CHUID signature check PIV Bio signature check 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 PIV Bio signature check 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*
PIV Authentication Key	Perform challenge and response with a PIV asymmetric key, and validate signature on response	Certificate validation of a PIV certificate	Possession of Card Match PIN or OCC data provided by Cardholder
Asymmetric Card Authentication Key	Perform challenge and response with a PIV asymmetric Card Authentication key, and validate signature on response	Certificate validation of a PIV certificate	Possession of Card
Symmetric Card Authentication Key	Perform challenge and response with a PIV symmetric key		Possession of Card
On-card Biometric Comparison	Establish Secure Messaging	Certificate validation of a PIV certificate	Possession of Card Match OCC data provided by Cardholder
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	Possession of Card

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.[26] For example, a relying party performing the authentication mechanism described in Appendix B.1.2 (Authentication using the PIV Authentication key) can expect to perform a challenge and response cryptographic authentication with a 2048-bit RSA key or an ECDSA (Curve P-256) key.

Deleted: 1) a 1024-bit RSA key, 2)

Deleted: ,

Deleted: 3)

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 mechanisms 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 key reference, and the PIV algorithm identifier as parameters of the command. The nonce is random data generated by the relying party and the 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 mechanism. The relying party, prior to issuing the challenge command, retrieved and parsed the X.509 certificate from the card in order to 1) validate the certificate and 2) extract the public key for the pending verification 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:[27]

Step 1: Algorithm Type Discovery:
The X.509 certificate stores the public key in the subjectPublicKeyInfo field. The subjectPublicKeyInfo data structure has an algorithm field, which includes an OID that identifies the public key's algorithm (RSA or ECC) as listed in Table 3-4 of SP 800-78.

Step 2: Key Size Discovery:
If the algorithm type, as determined in Step 1, is ECC then the key size is determined by the elliptic curve on which the key has been generated, which is P-256 for all elliptic curve PIV Authentication keys and Card Authentication keys.

If the algorithm type, as determined in Step 1, is RSA then the key size is determined by the public key's modulus. The public key appears in the subjectPublicKey field of subjectPublicKeyInfo and is encoded as a sequence that includes both the key's modulus and public exponent.

[26] Table 3-1, SP 800-78 lists the various algorithms and key sizes that may be used for each PIV key type.

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

As a final step, the discovered X.509 algorithm OID and key size are mapped to the PIV algorithm identifiers as defined in Table 6-2 of SP 800-78. 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 an 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 may be the Agency Code || System Code || Credential Number of the FASC-N or the Card UUID.

The symmetric Card Authentication key is optional to implement and a relying party has no prior knowledge of the key's existence. The following routine discovers the Card Authentication key's native implementation:

- Read the CHUID and either extract the Card UUID or extract the Agency Code || System code || Credential Number from the CHUID's FASC-N.

Deleted: or the Card UUID

- Retrieve the PIV algorithm identifier from the local lookup table. If no algorithm identifier is returned, authentication cannot be performed using the optional symmetric Card Authentication key either because the PIV Card does not implement the key or the local system cannot authenticate the response from the card.

C.3 PIV Algorithm Identifier Discovery for Secure Messaging

The Application Property Template, which is included in the response to the SELECT command, optionally includes a tag 0xAC, which indicates what cryptographic algorithms the PIV Card Application supports. The presence of algorithm identifier '27' or '2E' indicates that the corresponding cipher suite is supported by the PIV Card Application for secure messaging and that the PIV Card Application possesses a PIV Secure Messaging key of the appropriate size for the specified cipher suite.

Deleted: B

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., 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.

Authenticable 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 program running on a computer in communication with a card interface device.

Card Management Operation
Any operation involving the PIV Card Application Administrator.

Card Verifiable Certificate
A certificate stored on the card that includes a public key, the signature of a certification authority, and further information needed to verify the certificate.

Data Object
An item of information seen at the card command interface for which is specified a name, a description of logical content, a format, and a coding.

Key Reference
A key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. The identifier is part of the 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.

Paring Code — An 8 digit code used to establish a relationship between the PIV Card and a device for the purpose of creating the virtual contact interface after secure messaging has been established.

Deleted: 6 to

PIV Key Type — The type of a key. The PIV Key Types are 1) PIV Authentication key, 2) Card Authentication key, 3) digital signature key, 4) key management key, 5) retired key management key, 6) PIV Secure Messaging key, and 7) PIV 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

ACR	Access Control Rule
AID	Application Identifier
APDU	Application Protocol Data Unit
API	Application Programming Interface
ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
BER	Basic Encoding Rules
BIT	Biometric Information Template
CAK	Card Authentication Key
CBEFF	Common Biometric Exchange Formats Framework
CCC	Card Capability Container
CHUID	Card Holder Unique Identifier
CMS	Cryptographic Message Syntax
CVC	Card Verifiable Certificate
DER	Distinguished Encoding Rules
DG	Data Group
DTR	Derived Test Requirement
ECB	Electronic Code Book
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
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

HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
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
LRC	Longitudinal Redundancy Code
MAC	Message Authentication Code
MRTD	Machine Readable Travel Document
MSB	Most Significant Bit
NIST	National Institute of Standards and Technology
NPIVP	NIST Personal Identity Verification Program
OCC	On-Card biometric Comparison
OID	Object Identifier
OMB	Office of Management and Budget
PACS	Physical Access Control System
PIN	Personal Identification Number
PI	Person Identifier, a field in the FASC-N
PIV	Personal Identity Verification
PIX	Proprietary Identifier Extension
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PUK	PIN Unblocking Key
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
SM	Secure Messaging
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
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UUID	Universally Unique Identifier
VCI	Virtual Contact Interface

D.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'. The two hexadecimal digits are represented in quotations '2D' or as 0x2D. 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 RFU shall be set to 0.

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

The expression 'X' & 'Y' is a bitwise AND operation between bytes 'X' and 'Y'.

The symbol || means concatenation of byte strings. For example, if X is '00 01 02' and Y is '03 04 05', then X || Y is '00 01 02 03 04 05'.

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 other tables the M/O/C column identifies properties of the PIV Card Application that shall be present (M), may be present (O), or are conditionally required to be present (C).

BER-TLV data object tags are represented as byte sequences as described above. Thus, for example, 0x4F is the interindustry data object tag for an application identifier and 0x7F61 is the interindustry data object tag for the Biometric Information Templates Group Template.

Appendix E––References

[FIPS180] Federal Information Processing Standard 180-4, *Secure Hash Standard (SHS)*, March 2012. (See http://csrc.nist.gov)

[FIPS201] Federal Information Processing Standard 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013. (See http://csrc.nist.gov)

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

[IR7676] NIST Interagency Report 7676, *Maintaining and Using Key History on Personal Identity Verification (PIV) Cards*, June 2010. (See http://csrc.nist.gov)

[ISO7816] ISO/IEC 7816 (Parts 4, 5, 6, 8, and 9), *Information technology — Identification cards — Integrated circuit(s) cards with contacts.*

[ISO8824] ISO/IEC 8824-2:2002, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification.*

[ISO8825] 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).*

[MRTD] *ICAO 9303 Machine Readable Travel Documents, Part 3: Machine Readable Official Travel Documents, Volume 2: Specifications for Electronically Enabled MRtds with Biometric Identification Capability*, Third Edition – 2008. Published by authority of the Secretary General, International Civil Aviation Organization.

Deleted: *PKI for*

Deleted: *Offering ICC Read-Only Access Version - 1.1* Date - October 01, 2004

[NISTIR7863] NISTIR 7863, *Cardholder Authentication for the PIV Digital Signature Key*, NIST.

[PIV-I NFI] Personal Identity Verification Interoperability for Non-Federal Issuers, May 2009, or as amended. (See https://cio.gov/wp-content/uploads/downloads/2012/09/PIV_Interoperabillity_Non-Federal_Issuers_May-2009.pdf)

[PIV-I FAQ] Personal Identity Verification Interoperable (PIV-I) Frequently Asked Questions (FAQ), Version 1.0, June 28, 2010, or as amended. (See https://www.idmanagement.gov/sites/default/files/documents/PIV-I_FAQ.pdf)

[RFC2616] IETF RFC 2616, "Hypertext Transfer Protocol -- HTTP/1.1," June 1999. (See http://www.ietf.org/rfc/rfc2616.txt)

[RFC2585] IETF RFC 2585, "Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP," May 1999. (See http://www.ietf.org/rfc/rfc2585.txt)

[RFC4122] IETF RFC 4122, "A Universally Unique IDentifier (UUID) URN Namespace," July 2005. (See http://www.ietf.org/rfc/rfc4122.txt)

[RFC4530] IETF RFC 4530, “Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute,” June 2006. (See http://www.ietf.org/rfc/rfc4530.txt)

[RFC5280] IETF RFC 5280, “Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile,” May 2008. (See http://www.ietf.org/rfc/rfc5280.txt)

[RFC5652] IETF RFC 5652, “Cryptographic Message Syntax (CMS),” September 2009. (See http://www.ietf.org/rfc/rfc5652.txt)

[SP800-76] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013. (See http://csrc.nist.gov)

[SP800-78] Revised Draft NIST Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. (See http://csrc.nist.gov)

[SP800-87] NIST Special Publication 800-87 Revision 1, *Codes for Identification of Federal and Federally-Assisted Organizations*, April 2008. (See http://csrc.nist.gov)

[TIG SCEPACS] 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 Access Interagency Interoperability Working Group, July 30, 2004. (See https://www.idmanagement.gov/sites/default/files/documents/TIG_SCEPACS_v2.2_0.pdf)

Deleted: IETF,

Deleted: Draft

Deleted: June 2012

Deleted: http://fips201ep.cio.gov/documents/TIG_SCEPACS_v2.2.pdf