NIST Special Publication
NIST SP 800-73pt1-5 ipd

Interfaces for Personal Identity Verification

Part 1 – PIV Card Application Namespace, Data Model, and Representation

Initial Public Draft

Hildegard Ferraiolo
Ketan Mehta
Salvatore Francomacaro
Ramaswamy Chandramouli
Sarbari Gupta

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-73pt1-5.ipd

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-73pt1-5 ipd

Interfaces for Personal Identity Verification

Part 1 – PIV Card Application Namespace, Data Model, and Representation

Initial Public Draft

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

Sarbari Gupta
Electrosoft Services, Inc.

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-73pt1-5.ipd

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Certain commercial equipment, instruments, software, or materials, commercial or non-commercial, are identified in this paper in order to specify the experimental procedure adequately. Such identification does not imply recommendation or endorsement of any product or service by NIST, nor does it imply that the materials or equipment identified 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. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 et seq., Public Law (P.L.) 113-283. 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.

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.

NIST Technical Series Policies

Copyright, Use, and Licensing Statements
NIST Technical Series Publication Identifier Syntax

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be added on final publishing]
Supersedes NIST Series XXX (Month Year) DOI [Will be added on final publishing]

How to Cite this NIST Technical Series Publication:

Ferraiolo H, Mehta K, Francomacaro S, Chandramouli R, Gupta S (2023) Interfaces for Personal Identity Verification: Part 1 – PIV Card Application Namespace, Data Model, and Representation. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-73pt1-5 ipd. https://doi.org/10.6028/NIST.SP.800-73pt1-5.ipd

Author ORCID iDs

Hildegard Ferraiolo: 0000-0002-7719-5999
Ketan Mehta: 0009-0001-1191-8656
Salvatore Francomacaro: 0009-0009-0487-2520

Ramaswamy Chandramouli: 0000-0002-7387-5858
Sarbari Gupta: 0000-0003-1101-0856

Public Comment Period
September 27, 2023 – November 15, 2023

Submit Comments
piv_comments@nist.gov

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

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

FIPS 201 defines the requirements and characteristics of government-wide interoperable identity credentials. It specifies that these identity credentials must be stored on a smart card and that additional common identity credentials, known as derived PIV credentials, may be issued by a federal department or agency and used when a PIV Card is not practical. This document contains the technical specifications to interface with the smart card to retrieve and use 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 for the options and branches in international integrated circuit card standards. The specifications go further by constraining interpretations of the normative standards 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.

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.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: piv_comments@nist.gov

Configuration Management

When a federal agency adds one or several of the optional features listed in Appendix G to its PIV Cards, client applications must upgrade the PIV Middleware accordingly. This will enable the PIV Middleware to recognize and process the new data objects and/or features.

Where maximum interoperability is required, it is necessary to upgrade to SP 800-73-5-based PIV Middleware as they become available. Only SP 800-73-5-based PIV Middleware fully support all capabilities outlined in Appendix G. Previous versions of the PIV Middleware (based on SP 800-73-4 or older versions) are unaware of new SP 800-73-5 features and may have some limitations.

NPIVP Conformance Testing

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

- Validate the compliance and conformance of PIV Middleware and PIV Card Applications with the specifications in SP 800-73
- Provide assurance that the PIV Middleware and PIV Card Applications validated by NPIVP are interoperable

For further information on NPIVP, see https://csrc.nist.gov/projects/nist-personal-identity-verification-program.

With the final release of SP 800-73-5, NPIVP plans to revise and publish SP 800-85A-5, *PIV Card Application and Middleware Interface Test Guidelines*. This document will outline the Derived Test Requirements (DTRs) of SP 800-73-5 based PIV Card Applications and PIV Middleware. In parallel, NPIVP plans to update the test tools (Test Runner) for NPIVP laboratories to test PIV Card Applications in accordance with the DTRs in SP 800-85A-5. The Test Runner will not be updated for PIV Middleware testing because smart card support is natively supported by most endpoint devices. Hence, with this revision, SP 800-73-5 Part 3 is optional, and NPIVP conformance testing for PIV Middleware in accordance with SP 800-73 Part 3 is discontinued.

Once SP 800-85A-5 is published and the test tools are available to NPIVP test laboratories, SP 800-73-4 based testing will be discontinued, and SP 800-73-5-based testing will begin. NPIVP will announce the start of SP 800-73-5-based testing at https://csrc.nist.gov/projects/nist-personal-identity-verification-program/announcements.

Terminology

Throughout this publication the following terminology will be used:

- **SP 800-73-5** refers collectively to the three-part report, *Interfaces for Personal Identity Verification*.
- **SP 800-73-5 Part [#]** refers to a specific part of SP 800-73-5.

- The official citation that should be used when referencing a report can be found in the "How to Cite this NIST Technical Series Publication" in the front matter.

Table of Contents

182

183 ## List of Tables

List of Figures

Acknowledgments

The authors — Hildegard Ferraiolo, Ketan Mehta, Salvatore Francomacaro, and Ramaswamy Chandramouli of NIST and Sarbari Gupta of Electrosoft Services, Inc. — gratefully acknowledge the contributions of David Cooper, James Dray, William MacGregor, Scott Guthery, Teresa Schwarzhoff, and Jason Mohler, who co-authored prior versions of this three-part publication. 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.

1. Introduction

Homeland Security Presidential Directive-12 (HSPD-12) called for the adoption of a common identification standard to govern the interoperable use of identity credentials to allow physical and logical access to federally controlled facilities and information systems. In response, Federal Information Processing Standard (FIPS) 201 [FIPS201], *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed to define reliable, government-wide identity credentials for use in applications such as access to federally controlled facilities and information systems. FIPS 201 supports multiple types of authenticators, including authenticators on smart cards (also known as PIV Cards) and derived PIV credential authenticators in various other form factors. This publication contains technical specifications to interface with PIV Cards to retrieve and use identity credentials. Other specifications, such as NIST Special Publication (SP) 800-157r1 (Revision 1), contain procedures and life cycle activities to issue, maintain, and use derived PIV credentials.

1.1. Purpose

FIPS 201 defines processes for binding identities to authenticators, such as the PIV Card and derived PIV credentials used in the federal PIV system. SP 800-73-5 contains the technical specifications to interface with the PIV 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 for the options and branches in international integrated circuit card (ICC) standards [ISO7816]. The specifications go further by constraining interpretations of the normative standards to ease implementation, facilitate interoperability, and ensure performance in a manner tailored for PIV applications.

1.2. Scope

SP 800-73-5 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 ICCs CAN be used interchangeably by all information processing systems across federal agencies. SP 800-73-5 defines the PIV data elements' identifiers, structure, and format, as well as the client API and card command interface for use with the PIV Card.

This document — SP 800-73-5, *Interfaces for Personal Identity Verification: Part 1 – PIV Card Application Namespace, Data Model, and Representation* — is a companion document to FIPS 201 and specifies the PIV Card Application Namespace, the PIV Data Model, and its logical representation on the PIV Card.

1.3. Effective Date

These recommendations become effective upon final publication. New optional PIV Card features and deprecated PIV card features shall be phased in as part of new card stock acquisitions by federal department and agencies.

FIPS 201 compliance of PIV components and subsystems is provided in accordance with OMB [M-19-17] through products and services from the U.S. General Services Administration's (GSA) Interoperability Test Program and Approved Products and Services List.

1.4. Audience and Assumptions

This document is intended for 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) and are structured as follows:

- 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*, describes the data types found on the PIV client-application programming interface and the PIV Card Application card command interface.
- Appendix A provides container information for PIV Cards.
- Appendix B describes the PIV authentication mechanisms and is *informative*.
- Appendix C describes recommended procedures for key size and algorithm discovery and is *informative*.
- Appendix D provides the list of symbols, abbreviations and acronyms used in this document and is *informative*.
- Appendix E provides a glossary of terms and is *informative*.
- Appendix F describes the notation used in this document and is *informative*.
- Appendix G provides the revision history of the document and is *informative*.

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:

1. Proprietary Identifier eXtension (PIX) of the NIST Registered Application Provider IDentifier (RID)
2. ASN.1 object identifiers (OIDs) in the personal identity verification subset of the OIDs managed by NIST
3. 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 (i.e., without the two-byte version), as follows:

'A0 00 00 03 08 00 00 10 00'

3. PIV Data Model Elements

This section describes the data elements for the personal identity verification data model.

A PIV Card Application SHALL contain seven mandatory interoperable data objects, two conditionally mandatory data objects, and MAY contain 27 optional data objects. The seven mandatory data objects for interoperable use are:

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 27 optional data objects are:

- Printed Information
- Discovery Object
- Key History Object
- 20 retired X.509 Certificates for Key Management
- Cardholder Iris Images
- Biometric Information Templates Group Template
- Secure Messaging Certificate Signer
- 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 the 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 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. Other than the data model number, the contents of the CCC data elements are out of scope for this specification.

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

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 previously deprecated Authentication Key Map data element SHALL NOT be present in the CHUID.[1]
- 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 the person/organization association category MAY be populated with all zeros. The FASC-N SHALL NOT be modified post-issuance.

  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 of the PIV data objects that include the FASC-N. To eliminate unnecessary use of personally identifiable information, the FASC-N’s Person Identifier (PI) field SHOULD NOT encode Social Security numbers (SSNs). TIG SCEPACS also specifies PACS interoperability

[1] See Appendix G.

requirements in the tenth 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."

- 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 Card UUID SHALL NOT be modified post-issuance.
- 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 expiration date SHALL NOT be modified post-issuance.
- 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 Cardholder UUID SHALL NOT be modified post-issuance.
- 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.

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 of the CMS external digital signature in a content signing certificate, which SHALL be issued under the id-fpki-common-pivcontentSigning policy of [COMMON]. The content signing certificate SHALL also include an extended key usage (extKeyUsage) extension asserting id-PIV-contentsigning. The content signing certificate SHALL NOT expire before the expiration of the card authentication certificate.

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 that the certificate CAN be read without access control restrictions. The Public Key Infrastructure (PKI) cryptographic function (see **Table 5**) 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 that the certificate CAN be read without access control restrictions. The PKI cryptographic function (see **Table 5**) is under an "Always" access rule so 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.

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 [SP800-76].

3.1.6. Cardholder Facial Image

The facial image data object is used for automated facial authentication in attended and unattended modes (e.g., BIO or BIO-A), as well as automated facial authentication for PIV reissuance and verification data reset. The facial image data object MAY also be used for visual authentication by a guard (VIS). However, this authentication mechanism has been deprecated in accordance with FIPS 201-3. 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.

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 in the DataGroupHash. 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].

The card issuer's content signing 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 content signing certificate since it is included in the CHUID. At a minimum, unsigned data objects SHALL be included in the Security Object if present, such as the Printed Information data object. For maximum protection against credential splicing attacks (credential substitution), it is recommended, however, that all PIV data objects be included in the Security Object except for the PIV X.509 certificates and the Secure Messaging Certificate Signer data 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 that the certificate CAN be read without access control restrictions. The PKI cryptographic function (see **Table 5**) 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.[2]

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 that the certificate CAN be read without access control restrictions. The PKI cryptographic function (see **Table 5**) 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.

3.3. Optional Data Elements

When implemented, the 27 optional data elements of FIPS 201 SHALL conform to the specifications provided in this document.

3.3.1. Printed Information

All FIPS 201 mandatory information printed on the card is duplicated on the chip in that 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

If implemented, the Discovery Object is the 0x7E interindustry ISO/IEC 7816-6 template that nests interindustry data objects. For the Discovery Object, the 0x7E template nests two

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

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.

- 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 in two bytes:

  First byte: Bit 7 is set to 1 to indicate that the mandatory PIV Card Application PIN satisfies the PIV Access Control Rules (ACRs) for command execution[3] and data object access.

  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 OCC satisfies the PIV ACRs for command execution and PIV data object access.

  Bit 4 indicates whether the optional VCI is implemented.

  Bit 3 is set to zero if the pairing code is required to establish a VCI and is set to one if a VCI is established without a pairing code.

  Bits 8, 2, and 1 of the first byte SHALL be set to zero.

  Table 1 lists the acceptable values for the first byte of the PIN Usage Policy and summarizes the meaning of each value.

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

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

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

  Note: If Bit 6 of the first byte of the PIN Usage Policy is set to zero, then the second byte is RFU and SHALL be set to 0x00.

  PIV Card Applications that implement the VCI or for which the Global PIN or OCC satisfy the PIV ACRs for PIV data object access and command execution SHALL implement the Discovery Object.

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

591 **Table 1.** First byte of PIN Usage Policy discovery

Value	PIV Card Application PIN	Global PIN	OCC	VCI	Pairing Code Required
0x40	✓				
0x48	✓			✓	✓
0x4C	✓			✓	
0x50	✓		✓		
0x58	✓		✓	✓	✓
0x5C	✓		✓	✓	
0x60	✓	✓			
0x68	✓	✓		✓	✓
0x6C	✓	✓		✓	
0x70	✓	✓	✓		
0x78	✓	✓	✓	✓	✓
0x7C	✓	✓	✓	✓	

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

593 {'7E 12' {'4F 0B A0 00 00 03 08 00 00 10 00 01 00'} {'5F 2F 02 xx yy'}}, where xx and
594 yy encode the first and second byte of the PIN Usage Policy, as described in this section.

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

596 ### 3.3.3. Key History Object

597 Up to 20 retired key management private keys MAY be stored in the PIV Card Application. The
598 Key History object provides information about the retired key management private keys that are
599 present within the PIV Card Application.[4] Retired key management private keys are private keys
600 that correspond to X.509 Certificates for Key Management that have expired, have been revoked,
601 or have otherwise been superseded. The Key History object SHALL be present in the PIV Card
602 Application if the PIV Card Application contains any retired key management private keys but
603 MAY be present even if no such keys are present in the PIV Card Application. For each retired
604 key management private key in the PIV Card Application, the corresponding certificate MAY
605 either be present within the PIV Card Application or MAY only be available from an online
606 repository.

607 The Key History object includes two mandatory fields, *keysWithOnCardCerts* and
608 *keysWithOffCardCerts*, and one optional field, *offCardCertURL*. The *keysWithOnCardCerts*
609 field indicates the number of retired private keys within the PIV Card Application for which the
610 corresponding certificates are also stored within the PIV Card Application. The
611 *keysWithOffCardCerts* field indicates the number of retired private keys within the PIV Card
612 Application for which the corresponding certificates are not stored within the PIV Card
613 Application. The numeric values in both *keysWithOnCardCerts* and *keysWithOffCardCerts* are
614 represented as unsigned binary integers. The *offCardCertURL* field contains a URL that points to
615 a file containing the certificates that corresponding to all of the retired private keys within the
616 PIV Card Application, including those for which the corresponding certificate is also stored
617 within the PIV Card Application. The *offCardCertURL* field SHALL be present if the

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

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.[5] 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 that corresponding to only some of the retired key management private keys are available within the PIV Card Application, then the certificates that are stored in the PIV Card Application SHALL be the ones that were most recently issued.

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

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

3.3.4. Retired X.509 Certificates for Key Management

These objects hold the X.509 Certificates for Key Management that 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 that the certificates CAN be read without access control restrictions. The PKI cryptographic function (see **Table 5**) 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

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

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 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]. 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 5 of the first byte of the PIN Usage Policy SHALL be set. The BIT Group Template MAY be present when OCC does not satisfy the PIV ACRs for PIV data objects access but, if present, SHALL contain no BITs.[6] The Security Object enforces integrity of the BIT Group Template data object according to the issuer.

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 certificates needed to verify the signature on the secure messaging card verifiable certificate (CVC), as specified in SP 800-73-5 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 SP 800-73-5 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 201-3. 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[7] SHALL NOT be expired.

[6] A BIT Group Template with no BITs is encoded as '7F 61 03 02 01 00'.
[7] A valid PIV Card is defined as a PIV Card that is neither expired nor revoked.

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. A future version of SP 800-73 is expected to deprecate the Intermediate CVC data element.

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). The Security Object enforces the integrity of the Pairing Code Reference Data Container according to the issuer.

3.4. Inclusion of Universally Unique Identifiers (UUIDs)

This specification provides support for two UUIDs on a PIV Card. The Card UUID is unique for each card, and it SHALL be present on all PIV Cards. The Cardholder UUID 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 SHALL 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 and/or authentication using the secure messaging key, 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 SP 800-73-5 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].

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 as mandatory (M), optional (O), or conditional (C). The conditional data objects are the digital signature key and the 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.[8]

Table 2. Data Model Containers

Container Name	ContainerID	Access Rule for Read		M/O/C
		Contact	Contactless[9]	
Card Capability Container	0xDB00	Always	VCI	M
Card Holder Unique Identifier	0x3000	Always	Always	M
X.509 Certificate for PIV Authentication	0x0101	Always	VCI	M
Cardholder Fingerprints	0x6010	PIN	VCI and PIN	M
Security Object	0x9000	Always	VCI	M
Cardholder Facial Image	0x6030	PIN	VCI and PIN	M
X.509 Certificate for Card Authentication	0x0500	Always	Always	M
X.509 Certificate for Digital Signature	0x0100	Always	VCI	C
X.509 Certificate for Key Management	0x0102	Always	VCI	C
Printed Information	0x3001	PIN or OCC	VCI and (PIN or OCC)	O
Discovery Object	0x6050	Always	Always	O
Key History Object	0x6060	Always	VCI	O
Retired X.509 Certificate for Key Management 1	0x1001	Always	VCI	O
Retired X.509 Certificate for Key Management 2	0x1002	Always	VCI	O
Retired X.509 Certificate for Key Management 3	0x1003	Always	VCI	O
Retired X.509 Certificate for Key Management 4	0x1004	Always	VCI	O
Retired X.509 Certificate for Key Management 5	0x1005	Always	VCI	O

[8] 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. In addition, the asymmetric CAK needs to be generated off-card and loaded onto both chips for dual chip implementations.

[9] The term "virtual contact interface (VCI)" is used in this document as shorthand for the following security condition: (command is submitted over secure messaging) AND (the Discovery Object is present) AND (Bit 4 of the first byte of the PIN Usage Policy is one) AND ((the security status indicator associated with the pairing code is TRUE) OR (Bit 3 of the first byte of the PIN Usage Policy is one)).

Container Name	ContainerID	Access Rule for Read		M/O/C
		Contact	Contactless[9]	
Retired X.509 Certificate for Key Management 6	0x1006	Always	VCI	O
Retired X.509 Certificate for Key Management 7	0x1007	Always	VCI	O
Retired X.509 Certificate for Key Management 8	0x1008	Always	VCI	O
Retired X.509 Certificate for Key Management 9	0x1009	Always	VCI	O
Retired X.509 Certificate for Key Management 10	0x100A	Always	VCI	O
Retired X.509 Certificate for Key Management 11	0x100B	Always	VCI	O
Retired X.509 Certificate for Key Management 12	0x100C	Always	VCI	O
Retired X.509 Certificate for Key Management 13	0x100D	Always	VCI	O
Retired X.509 Certificate for Key Management 14	0x100E	Always	VCI	O
Retired X.509 Certificate for Key Management 15	0x100F	Always	VCI	O
Retired X.509 Certificate for Key Management 16	0x1010	Always	VCI	O
Retired X.509 Certificate for Key Management 17	0x1011	Always	VCI	O
Retired X.509 Certificate for Key Management 18	0x1012	Always	VCI	O
Retired X.509 Certificate for Key Management 19	0x1013	Always	VCI	O
Retired X.509 Certificate for Key Management 20	0x1014	Always	VCI	O
Cardholder Iris Images	0x1015	PIN	VCI and PIN	O
Biometric Information Templates Group Template	0x1016	Always	Always	O
Secure Messaging Certificate Signer	0x1017	Always	Always	O
Pairing Code Reference Data Container	0x1018	PIN or OCC	VCI and (PIN or OCC)	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 800-73-5 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 that has a specified 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 as well 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]. However, tag values of the PIV data object's inner tag assignments do not conform to BER-TLV requirements[10] 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.

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'.

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**.

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

[10] 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.

771 OID of the CHUID on the PIV client-application programming interface is
772 "2.16.840.1.101.3.7.2.48.0."

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

776 **Table 2** lists the ACRs of the thirty-six PIV Card Application data objects.

777 **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

Data Object for Interoperable Use	ASN.1 OID	BER-TLV Tag	M/O/C
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

778

5. Data Types and Their Representation

This section describes the data types used in the PIV Client Application Programming Interface (SP 800-73-5, Part 3) and PIV Card Command Interface (SP 800-73-5, 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.

5.1. Key References

A key reference is a 1-byte reference data identifier that specifies a cryptographic key or PIN according to its PIV Key Type. **Table 4**, **Table 5**, and SP 800-78, Table 8, define the key reference values that SHALL be used on the PIV interfaces. For example, the key reference values are used in a cryptographic protocol, such as an authentication or a signing protocol. Key references are only assigned to private and secret (symmetric) keys, PINs, PIN Unblocking Keys (PUKs), OCC, and the pairing code. All other PIV Card Application key reference values are reserved for future use.

In accordance with FIPS 201, no more than 10 consecutive activation retries for each of the activation methods (i.e., PIN and OCC attempts) SHALL be permitted. Issuers MAY further restrict the maximum retry limit to a lower value, as indicated in **Table 4** below.

Table 4. PIV Card Application authentication data references

Key Reference Value	PIV Reference Data Type	Authenticable Entity	Security Condition for Use		Retry Counter Value	Number of Unblocks
			Contact	Contactless		
'00'	Global PIN	Cardholder	Always	VCI	10 or lower	Platform Specific
'80'	PIV Card Application PIN	Cardholder	Always	VCI	10 or lower	Issuer Specific
'81'	PIN Unblocking Key	PIV Card Application Administrator	Always	Never	Issuer Specific	Issuer Specific
'96'	Primary Finger OCC	Cardholder	Always	SM	10 or lower	Issuer Specific
'97'	Secondary Finger OCC	Cardholder	Always	SM	10 or lower	Issuer Specific
'98'	Pairing Code	Cardholder	Always[11]	SM	Issuer Specific	Issuer Specific

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

799 **Table 5.** PIV Card Application key references

Key Reference Value (i.e., Key ID)	PIV Key Type	Administrator	Security Condition for Use	
			Contact	Contactless
'04'	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[12]	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)

800 Secure messaging (SM) is defined in Section 5.4, and VCI is defined in Section 5.5. Table 2 of
801 SP 800-73-5 Part 2 specifies the security conditions for each command.

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

805 The access control rules for PIV data object access SHALL reference the PIV Card Application
806 PIN and MAY optionally reference the cardholder Global PIN or OCC data. If the Global PIN is
807 used by the PIV Card Application, then the Global PIN format SHALL follow the PIV Card
808 Application PIN format defined in Section 2.4.3 of SP 800-73-5 Part 2.

809 PIV Card Applications with the Discovery Object and Bit 6 of the first byte of the PIN Usage
810 Policy value set to one, as per Section 3.3.2, SHALL reference the PIV Card Application PIN
811 and the cardholder Global PIN in the access control rules for PIV data object access.
812 Additionally, the PIV Card Application card commands CAN change the status of the Global
813 PIN and MAY change its reference data while the PIV Card Application is the currently selected
814 application.

[12] 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. However, the use of the symmetric card authentication key has been deprecated in FIPS 201-3 and may be removed in a future version of the standard.

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]. The fingerprints used for OCC MAY be taken from the full set of fingerprints collected for PIV background investigations and SHOULD be imaged from fingers not imaged for off-card one-to-one comparison.

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 5**) 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.

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 SP 800-73-5 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.

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 (i.e., 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.[13]

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

[13] 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 when determining the method by which they provide cardholders with the values of their pairing codes.

to communicate with a PIV Card over its virtual contact interface obtain the card's pairing code during a registration step 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 code until the card expires.[14] 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 1-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 9 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 6**. These identifiers serve as inputs to the GENERATE ASYMMETRIC KEY PAIR card command and the SP 800-73-5 Part 3 pivGenerateKeyPair() client API function call, which initiates the generation and storage of the asymmetric key pair.

Table 6. Cryptographic mechanism identifiers

Cryptographic Mechanism Identifier	Description	Parameter
'05'	RSA 3072	Optional public exponent encoded big-endian
'07'	RSA 2048	Optional public exponent encoded big-endian
'11'	ECC: Curve P-256	None
'14'	ECC: Curve P-384	None

Higher strength keys are recommended per SP 800-56 Part 1 starting in 2031. See SP 800-78-5, Tables 9 and 10, which reflect support for higher strength keys for PIV cards and supporting systems, where applicable.

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

[14] As noted in Section 5.5, the pairing code does not need to be submitted if the Bit 3 of the first byte of the PIN Usage Policy is set to one.

5.4. Secure Messaging and Authentication Using a Secure Messaging Key (SM-AUTH)

A PIV Card Application MAY optionally support 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. The symmetric session keys 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.

If implemented, SM for non-card management operations SHALL only be established using the PIV Secure Messaging key specified in **Table 5** and the SM protocol in accordance with the specifications in Section 4 of SP 800-73-5 Part 2.

A PIV Card Application may optionally support authentication using the Secure Messaging key (SM-AUTH). When SM-AUTH is supported, the PIV Card and therefore the cardholder is authenticated to the relying system.

5.5. Virtual Contact Interface

The term "virtual contact interface (VCI)" is used in this document as shorthand for a security condition. As described in access control rules in this document and in SP 800-73-5 Part 2, all non-card management operations that are allowed over the contact interface MAY be carried out over the contactless interface if the VCI security condition is satisfied. Support for the VCI is optional.

The VCI security condition supports two different configurations for the establishment of the VCI. In the default (and recommended) configuration, the VCI is only established after both secure messaging has been established and the pairing code has been presented to the card using secure messaging. In the non-default configuration, the VCI is established through secure messaging without any further steps.

The VCI security condition is:

> (command is submitted over secure messaging) **AND** (the Discovery Object is present) **AND** (Bit 4 of the first byte of the PIN Usage Policy is one) **AND** ((the security status indicator associated with the pairing code is TRUE) **OR** (Bit 3 of the first byte of the PIN Usage Policy is one))

PIV Card Applications that support the VCI SHALL support the configuration in which Bit 3 of the first byte of the PIN Usage Policy is set to zero (i.e., the configuration in which submission of the pairing code to the PIV Card Application is required to establish the VCI) and MAY additionally support the configuration in which Bit 3 of the first byte of the PIN Usage Policy is set to one. Card management systems (CMS) SHALL be configured to set Bit 3 of the first byte of the PIN Usage Policy to zero by default whenever the Discovery Object is present.

Requiring that the pairing code be submitted to the PIV Card Application in order to establish the VCI protects the previously contact-restricted X.509 certificates from skimming[15] and also

[15] Skimming is when data is surreptitiously obtained from a contactless card using a hidden reader that powers, commands, and reads from the card within the maximum read distance (reported as about 25 cm with ISO/IEC 14443 smart cards like the PIV Card).

protects PIN-based card activation from being blocked. While it is recommended that the default configuration of CMSs remain unchanged, the configuration of a CMS MAY be changed to set Bit 3 of the first byte of the PIN Usage Policy to one (i.e., to configure PIV Cards to establish VCIs without the submission of a pairing code) if the configuration change is approved by the designated approving authority (DAA) and if compensating controls are implemented to ensure that personally identifiable information (e.g., name, email address, and organization) CANNOT be skimmed from the PIV Card when in close proximity when the card is outside of its protective sleeve.

A DAA's decision to approve the issuance of PIV Cards that implement the VCI without requiring the pairing code SHALL be based on a risk assessment that weighs the perceived benefit against the risk of unauthorized disclosure of cardholder data exposing previously contact-restricted X.509 certificates to skimming. The previously contact-restricted X.509 certificates include information about the cardholder, such as name and email address. Compensating controls SHALL be captured in the appropriate system security plan.[16] Systems that accept externally issued PIV Cards SHALL be able to accept PIV Cards with either VCI configuration.

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 7**. The descriptions of individual card commands provide additional information for interpreting returned status words.

Table 7. 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

[16] See SP 800-18r1, Guide for Developing Security Plans for Federal Information Systems.

References

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 2.4, April 2023 [or as amended]. Available at https://www.idmanagement.gov/docs/fpki-x509-cert-policy-common.pdf

[FIPS180] National Institute of Standards and Technology (2015) Secure Hash Standard (SHS). (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 180-4 [or as amended]. https://doi.org/10.6028/NIST.FIPS.180-4

[FIPS201] National Institute of Standards and Technology (2022) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-3. https://doi.org/10.6028/NIST.FIPS.201-3

[GSC-IS] Schwarzhoff TT, Dray JF, Jr., Wack JP, Dalci E, Goldfine A, Iorga M (2003) Government Smart Card Interoperability Specification, Version 2.1. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 6887, 2003 Edition [or as amended]. https://doi.org/10.6028/NIST.IR.6887e2003

[IR7676] Cooper DA (2010) Maintaining and Using Key History on Personal Identity Verification (PIV) Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7676. https://doi.org/10.6028/NIST.IR.7676

[IR7863] Polk WT, Ferraiolo H, Cooper DA (2015) Cardholder Authentication for the PIV Digital Signature Key. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7863. Available at https://doi.org/10.6028/NIST.IR.7863

[ISO7816] International Organization for Standardization/International Electrotechnical Commission (2004-2020) ISO/IEC 7816 — Identification cards — Integrated circuit cards. (multiple parts):

- International Organization for Standardization/International Electrotechnical Commission (2020) ISO/IEC 7816-4:2020 — Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/77180.html
- International Organization for Standardization/International Electrotechnical Commission (2004) ISO/IEC 7816-5:2004 — Identification cards — Integrated circuit cards — Part 5: Registration of application providers. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/34259.html
- International Organization for Standardization/International Electrotechnical Commission (2016) ISO/IEC 7816-6:2016 — Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange. (International Organization for Standardization,

Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/64598.html

- International Organization for Standardization/International Electrotechnical Commission (2016) ISO/IEC 7816-8:2021 — Identification cards — Integrated circuit cards — Part 8: Commands and mechanisms for security operations. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/79893.html
- International Organization for Standardization/International Electrotechnical Commission (2017) ISO/IEC 7816-9:2017 — Identification cards — Integrated circuit cards — Part 9: Commands for card management. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/67802.html

[ISO8824] International Organization for Standardization/International Electrotechnical Commission (2021) ISO/IEC 8824-2:2021 — Information technology — Abstract Syntax Notation One (ASN.1) – Part 2: Information object specification. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/81417.html

[ISO8825] International Organization for Standardization/International Electrotechnical Commission (2015) ISO/IEC 8825-1:2015 — Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER) Part 1. (International Organization for Standardization, Geneva, Switzerland) [or as amended]. Available at https://www.iso.org/standard/81420.html

[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, Eighth Edition, 2021. Published by authority of the Secretary General, International Civil Aviation Organization.

[RFC2616] Fielding R, Gettys J, Mogul J, Frstk H, Masinter L, Leach P, Berners-Lee T (1999) Hypertext Transfer Protocol -- HTTP/1.1. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 2616. https://doi.org/10.17487/RFC2616

[RFC2585] Housley R, Hoffman P (1999) Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 2585. https://doi.org/10.17487/RFC2585

[RFC4122] Leach P, Mealling M, Salz R (2005) A Universally Unique IDentifier (UUID) URN Namespace. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 4122. https://doi.org/10.17487/RFC4122

[RFC4530] Zeilenga K, (2006) Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 4530. https://doi.org/10.17487/RFC4530

[RFC5280] Cooper D, Santesson S, Farrell S, Boeyen S, Housley R, Polk W (2008) Internet X.509 Public Key Infrastructure Certification and Certificate Revocation List (CRL) Profile. (Internet Engineering Task Force (IETF)), IETF Request for Comments (RFC) 5280. https://doi.org/10.17487/RFC5280

[RFC5652] IETF RFC 5652, "Cryptographic Message Syntax (CMS)," September 2009. https://doi.org/10.17487/RFC5652

[SP800-76] Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-76-2

[SP800-78] Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4 [or as amended]. https://doi.org/10.6028/NIST.SP.800-78-4

[SP800-85A-4] Cooper D, Ferraiolo H, Chandramouli R, Mohler J (2016) PIV Card Application and Middleware Interface Test Guidelines (SP 800-73-4 Compliance). (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-85A-4 [or as amended]. https://doi.org/10.6028/NIST.SP.800-85A-4

[SP800-87] Ferraiolo H (2018) Codes for Identification of Federal and Federally-Assisted Organizations. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-87, Rev. 2 [or as amended]. https://doi.org/10.6028/NIST.SP.800-87r2

[TIG SCEPACS] PACS v2.2, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.3, The Government Smart Card Interagency Advisory Board's Physical Access Interagency Interoperability Working Group, December 2005. https://www.idmanagement.gov/docs/pacs-tig-scepacs.pdf

Appendix A. PIV Data Model

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

The SP 800-73-5 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 with information regarding which interface is in use. In the dual-chip configuration, a separate PIV Card Application SHALL be loaded on each chip.

Table 8. PIV data containers

Container Description	ContainerID	BER-TLV Tag	Container Minimum Capacity (Bytes)[17]	Access Rule for Read		M/O/C
				Contact	Contactless	
Card Capability Container	0xDB00	'5FC107'	170	Always	VCI	M
Card Holder Unique Identifier	0x3000	'5FC102'	2881	Always	Always	M
X.509 Certificate for PIV Authentication (Key Reference '9A')	0x0101	'5FC105'	1857	Always	VCI	M
Cardholder Fingerprints	0x6010	'5FC103'	4006	PIN	VCI and PIN	M
Security Object	0x9000	'5FC106'	1336	Always	VCI	M
Cardholder Facial Image	0x6030	'5FC108'	12710	PIN	VCI and PIN	M
X.509 Certificate for Card Authentication (Key Reference '9E')	0x0500	'5FC101'	1857	Always	Always	M
X.509 Certificate for Digital Signature (Key Reference '9C')	0x0100	'5FC10A'	1857	Always	VCI	C
X.509 Certificate for Key Management (Key Reference '9D')	0x0102	'5FC10B'	1857	Always	VCI	C
Printed Information	0x3001	'5FC109'	245	PIN or OCC	VCI and (PIN or OCC)	O
Discovery Object	0x6050	'7E'	19	Always	Always	O
Key History Object	0x6060	'5FC10C'	128	Always	VCI	O
Retired X.509 Certificate for Key Management 1 (Key reference '82')	0x1001	'5FC10D'	1895	Always	VCI	O

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

Container Description	ContainerID	BER-TLV Tag	Container Minimum Capacity (Bytes)[17]	Access Rule for Read		M/O/C
				Contact	Contactless	
Retired X.509 Certificate for Key Management 2 (Key reference '83')	0x1002	'5FC10E'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 3 (Key reference '84')	0x1003	'5FC10F'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 4 (Key reference '85')	0x1004	'5FC110'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 5 (Key reference '86')	0x1005	'5FC111'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 6 (Key reference '87')	0x1006	'5FC112'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 7(Key reference '88')	0x1007	'5FC113'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 8(Key reference '89')	0x1008	'5FC114'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 9 (Key reference '8A')	0x1009	'5FC115'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 10 (Key reference '8B')	0x100A	'5FC116'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 11 (Key reference '8C')	0x100B	'5FC117'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 12 (Key reference '8D')	0x100C	'5FC118'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 13 (Key reference '8E')	0x100D	'5FC119'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 14 (Key reference '8F')	0x100E	'5FC11A'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 15 (Key reference '90')	0x100F	'5FC11B'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 16 (Key reference '91')	0x1010	'5FC11C'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 17 (Key reference '92')	0x1011	'5FC11D'	1895	Always	VCI	O

Container Description	ContainerID	BER-TLV Tag	Container Minimum Capacity (Bytes)[17]	Access Rule for Read		M/O/C
				Contact	Contactless	
Retired X.509 Certificate for Key Management 18 (Key reference '93')	0x1012	'5FC11E'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 19 (Key reference '94')	0x1013	'5FC11F'	1895	Always	VCI	O
Retired X.509 Certificate for Key Management 20 (Key reference '95')	0x1014	'5FC120'	1895	Always	VCI	O
Cardholder Iris Images	0x1015	'5FC121'	7106	PIN	VCI and PIN	O
Biometric Information Templates Group Template	0x1016	'7F61'	65	Always	Always	O
Secure Messaging Certificate Signer	0x1017	'5FC122'	2471	Always	Always	O
Pairing Code Reference Data Container	0x1018	'5FC123'	12	PIN or OCC	VCI and (PIN or OCC)	O

Note that all data elements of the following data objects are mandatory unless specified as optional or conditional. Also note that in all tables that follow, the values in the “Max. Bytes” columns denote the lengths of the value (V) fields of BER-TLV elements.

Table 9. 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
Error Detection Code	0xFE	LRC	0

Note that he previously deprecated optional Extended Application CardURL and Security Object Buffer data elements have been eliminated in this version of SP 800-73.

1068 **Table 10.** Card Holder Unique Identifier

Card Holder Unique Identifier		0x3000	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
FASC-N	0x30	Fixed	25
GUID	0x34	Fixed	16
Expiration Date	0x35	Date (YYYYMMDD)	8
Cardholder UUID (Optional)	0x36	Fixed	16
Issuer Asymmetric Signature	0x3E	Variable	2816[18]
Error Detection Code	0xFE	LRC	0

1069 Note that the Buffer Length, Organizational Identifier, and DUNS data elements have been
1070 eliminated in this version of SP 800-73.

1071 The Error Detection Code is the same element as the Longitudinal Redundancy Code (LRC) in
1072 [TIG SCEPACS]. It is present in the CHUID because TIG SCEPACS makes the LRC
1073 mandatory. However, this document makes no use of the Error Detection Code, and therefore the
1074 length of the TLV value is set to 0 bytes (i.e., no value will be supplied).

1075 **Table 11.** X.509 Certificate for PIV Authentication

X.509 Certificate for PIV Authentication		0x0101	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Certificate	0x70	Variable	1856[19]
CertInfo	0x71	Fixed	1
Error Detection Code	0xFE	LRC	0

1076 Note that the MSCUID data element has been eliminated in this version.

1077 **Table 12.** Cardholder fingerprints

Cardholder Fingerprints		0x6010	
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Fingerprint I & II	0xBC	Variable	4000[20]
Error Detection Code	0xFE	LRC	0

1078 **Table 13.** 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

1079

[18] The values in the "Max. Bytes" columns denote the lengths of the value (V) fields of BER-TLV elements.
[19] This is the recommended length. The certificate size can exceed the indicated length value.
[20] This is the 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. For the latter, the "Max. Bytes" value quoted is a recommendation, and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the "Max. Bytes." Note that the use of separate content signing keys for biometric data and CHUID has been deprecated in FIPS 201-3. In future revisions, the CHUID and biometric elements will be signed with the same key. The content signing certificate will not be found in this data element but instead will be contained in the CHUID data element. Hence, the size will be as indicated in the table.

1080 **Table 14.** Cardholder facial image

Cardholder Facial Image	0x6030		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Facial Image	0xBC	Variable	12704[21]
Error Detection Code	0xFE	LRC	0

1081 **Table 15.** 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

1082 Agencies SHOULD use tags 0x02, 0x07 and 0x08 to successfully match the printed information
1083 for verification on Zone 8F (Employee Affiliation) and Zone 10F (Agency, Department, or
1084 Organization) on the face of the card with the printed information stored electronically on the
1085 card.

1086 **Table 16.** X.509 Certificate for Digital Signature

X.509 Certificate for Digital Signature	0x0100		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Certificate	0x70	Variable	1856[22]
CertInfo	0x71	Fixed	1
Error Detection Code	0xFE	LRC	0

1087 Note that the MSCUID data element has been eliminated in this version.

1088 **Table 17.** X.509 Certificate for Key Management

X.509 Certificate for Key Management	0x0102		
Certificate	0x70	Variable	1856[22]
CertInfo	0x71	Fixed	1
Error Detection Code	0xFE	LRC	0

[21] This is the recommended length. The certificate that signed the Facial Image data element (tag 0xBC) can be stored in the CHUID or in the Facial Image data element itself. For the latter, the "Max. Bytes" value quoted is a recommendation, and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the "Max. Bytes." Note that the use of separate content signing keys for biometric data and CHUID has been deprecated in FIPS 201-3. In future revisions, the CHUID and biometric elements will be signed with the same key. The content signing certificate will not be found in this data element but instead will be contained in the CHUID data element. Hence, the size will be as indicated in the table.

[22] This is the recommended length. The certificate size can exceed the indicated length value.

Note that the MSCUID data element has been eliminated in this version.

Table 18. X.509 Certificate for Card Authentication

X.509 Certificate for Card Authentication	0x0500		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Certificate	0x70	Variable	1856[23]
CertInfo	0x71	Fixed	1
Error Detection Code	0xFE	LRC	0

Note that the MSCUID data element has been eliminated in this version of SP 800-73.

Table 19. Discovery Object

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

Table 20. Key History Object

Key History Object	0x6060		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
keysWithOnCardCerts	0xC1	Fixed	1
keysWithOffCardCerts	0xC2	Fixed	1[24]
offCardCertURL (Conditional)[25]	0xF3	Variable	118
Error Detection Code	0xFE	LRC	0

Table 21. 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[23]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Note that the optional MSCUID data element was deprecated in a previous version and eliminated in this version of SP 800-73. However, historic retired key management certificates MAY still include the MSCUID element, so it is retained as an optional data element above. This applies to all of the retired key management key objects represented in **Table 21** - **Table 40**.

[23] This is the recommended length. The certificate size can exceed the indicated length value.
[24] The numeric values indicated in keysWithOnCardCerts and keysWithOffCardCerts are represented as unsigned binary integers.
[25] 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.

1099 **Table 22.** 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[26]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1100 **Table 23.** 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[26]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1101 **Table 24.** 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[26]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1102 **Table 25.** 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[26]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1103 **Table 26.** 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[26]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1104 **Table 27.** 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[26]
CertInfo	0x71	Fixed	1

[26] This is the recommended length. The certificate size can exceed the indicated length value.

Retired X.509 Certificate for Key Management 7	0x1007		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 28. 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[27]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 29. 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[27]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 30. 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[27]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 31. 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[27]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 32. 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[27]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

[27] This is the recommended length. The certificate size can exceed the indicated length value.

1110 **Table 33.** 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1111 **Table 34.** 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1112 **Table 35.** 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1113 **Table 36.** 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1114 **Table 37.** 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

1115 **Table 38.** 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[28]
CertInfo	0x71	Fixed	1

[28] This is the recommended length. The certificate size can exceed the indicated length value.

Retired X.509 Certificate for Key Management 18	0x1012		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 39. 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

Table 40. 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[28]
CertInfo	0x71	Fixed	1
MSCUID (Optional)	0x72	Variable	38
Error Detection Code	0xFE	LRC	0

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

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.[29] CompressionTypeLsb and IsX509 SHALL be set to 0 for PIV Card Applications. Thus, for a certificate encoded in uncompressed form, CertInfo SHALL be 0x00. For a certificate encoded using GZIP compression, CertInfo SHALL be 0x01.

Table 41. Cardholder iris images

Cardholder Iris Images	0x1015		
Data Element (TLV)	**Tag**	**Type**	**Max. Bytes**
Images for Iris	0xBC	Variable	7100[30]
Error Detection Code	0xFE	LRC	0

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

[30] This is the 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. For the latter, the "Max. Bytes" value quoted is a recommendation, and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the "Max. Bytes." Note that the use of separate content signing keys for biometric data and CHUID has been deprecated in FIPS 201-3. In future revisions, the CHUID and biometric elements will be signed with the same key. The content signing certificate will not be found in this data element but instead will be contained in the CHUID data element. Hence, the size will be as indicated in the table

1128 **Table 42.** 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

1129 **Table 43.** 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)[31]	0x7F21	Variable	601
Error Detection Code	0xFE	LRC	0

1130 The CertInfo byte in the Secure Messaging Certificate Signer data object SHALL provide
1131 information about the X.509 Certificate for Content Signing. The Intermediate CVC, if present,
1132 shall be stored in uncompressed form.

1133 **Table 44.** 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

1134

[31] 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

PIV authentication mechanisms and application scenarios are described in this section to provide guidelines on the usage and behavior supported by the PIV Card. FIPS 201 describes PIV authentication as "the process of establishing confidence in the identity of the cardholder presenting a PIV Card" [FIPS201]. 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, per Section 4.1.2 of FIPS 201
  - Use of cryptographic challenge-response schemes with symmetric keys
  - Use of asymmetric authentication schemes to validate private keys embedded within the PIV Card
- Credential Validation (CredV) — This is the process of verifying the various types of credentials (e.g., visual credentials, biometrics, and certificates) held by the PIV Card. Credential validation mechanisms include:
  - Verification of certificates on the PIV Card
  - Verification of signatures on the PIV biometrics and the CHUID
  - Checking the expiration date
  - Checking the revocation status of the credentials on the PIV Card
  - Visual inspection of PIV Card visual elements[32] (e.g., the photo, the printed name, rank).
- Cardholder Validation (HolderV) — This is the process of establishing that the PIV Card is in the possession of the individual to whom the card was 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 live fingerprint, facial image, 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 PIN provided with the PIN on the PIV Card

[32] This has been deprecated per FIPS 201-3.

- Matching the live fingerprint, facial image, or iris image samples provided by the cardholder with the biometric information embedded within the PIV Card
- Matching the visual characteristics of the cardholder with the photo on the PIV Card[33]

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.

[33] Use of the photo on the PIV Card for visual authentication has been deprecated in FIPS 201-3 and may be removed from a future edition of the standard.

B.1.1. Authentication Using PIV Biometrics (BIO)

Figure 1 shows the general authentication mechanism that uses PIV biometrics for off-card matching.

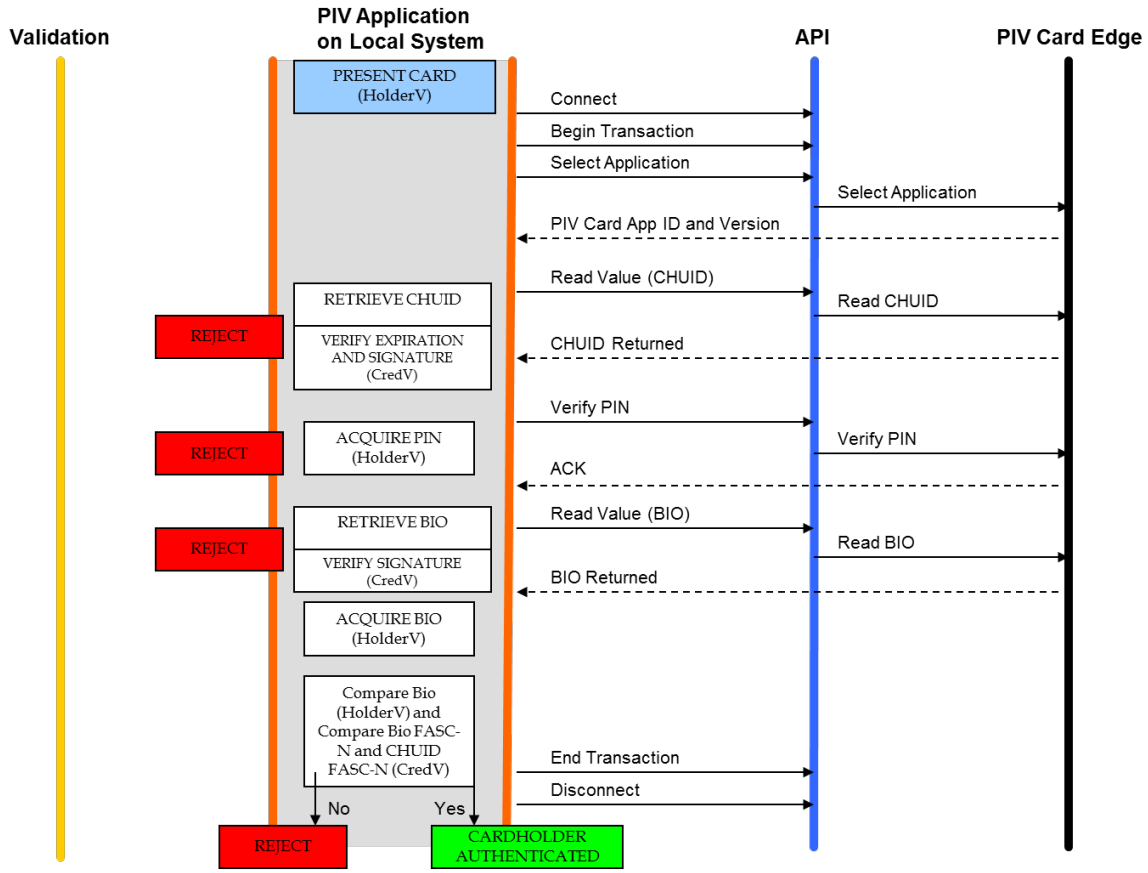

Fig. 1. Authentication using PIV Biometrics (BIO)

The assurance of authentication using PIV biometrics 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 **Fig. 2**.

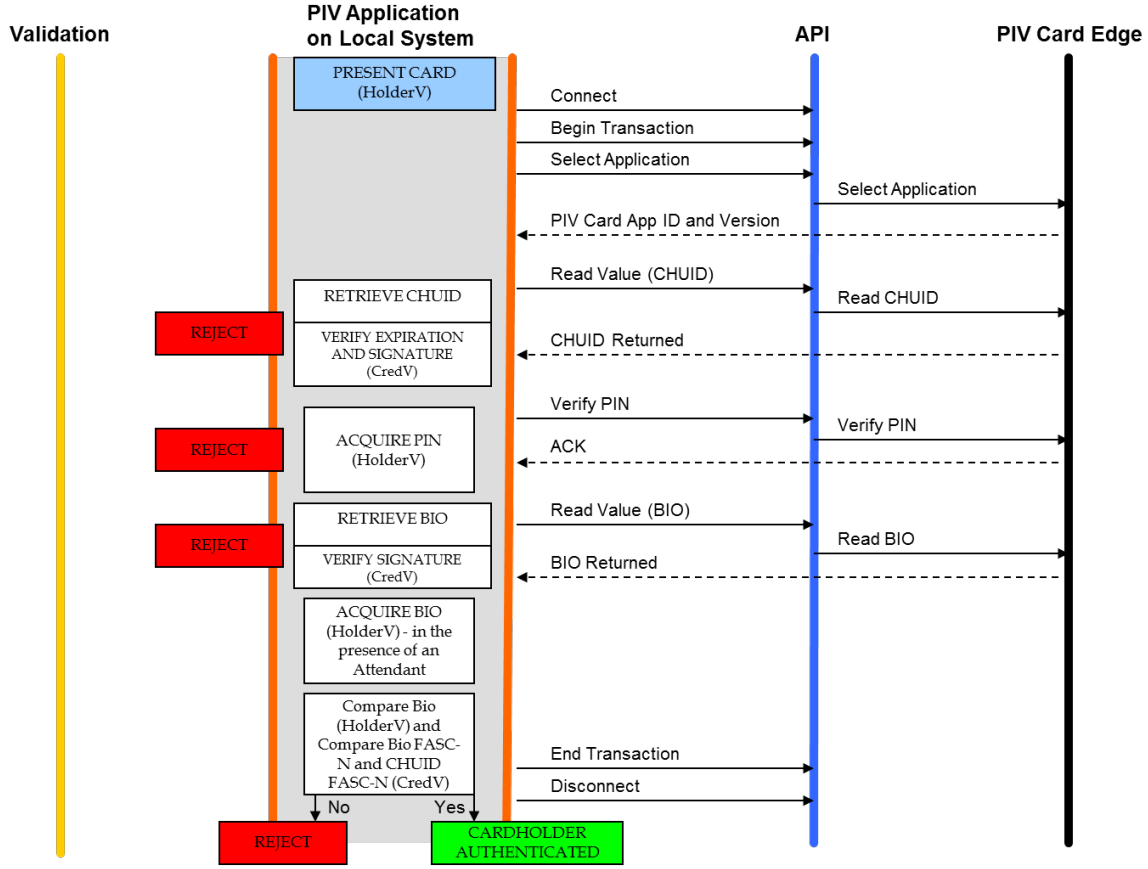

Fig. 2. Authentication using PIV Biometrics Attended (BIO-A)

B.1.2. Authentication Using PIV Authentication Key

Figure 3 shows the authentication mechanism using the PIV Authentication key.

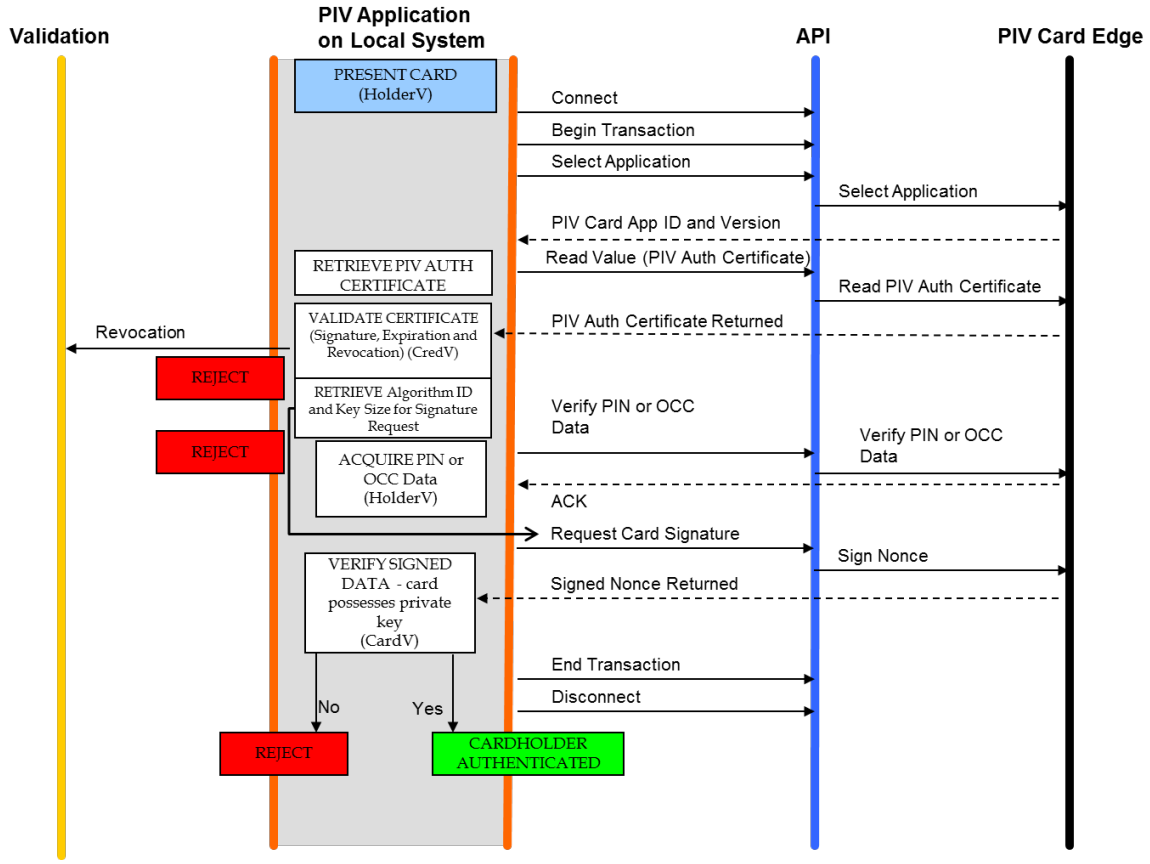

Fig. 3. Authentication using PIV Authentication Key

B.1.3. Authentication Using Card Authentication Key

Authentication mechanisms using the Card Authentication key are illustrated in **Fig. 4** and **Fig. 5**. **Figure 4** illustrates the use of the mandatory asymmetric Card Authentication key, while **Fig. 5** uses the deprecated, optional symmetric Card Authentication key for the authentication mechanism. Note that the symmetric card authentication key has been deprecated in FIPS 201-3 and MAY be removed in a future version of the standard.

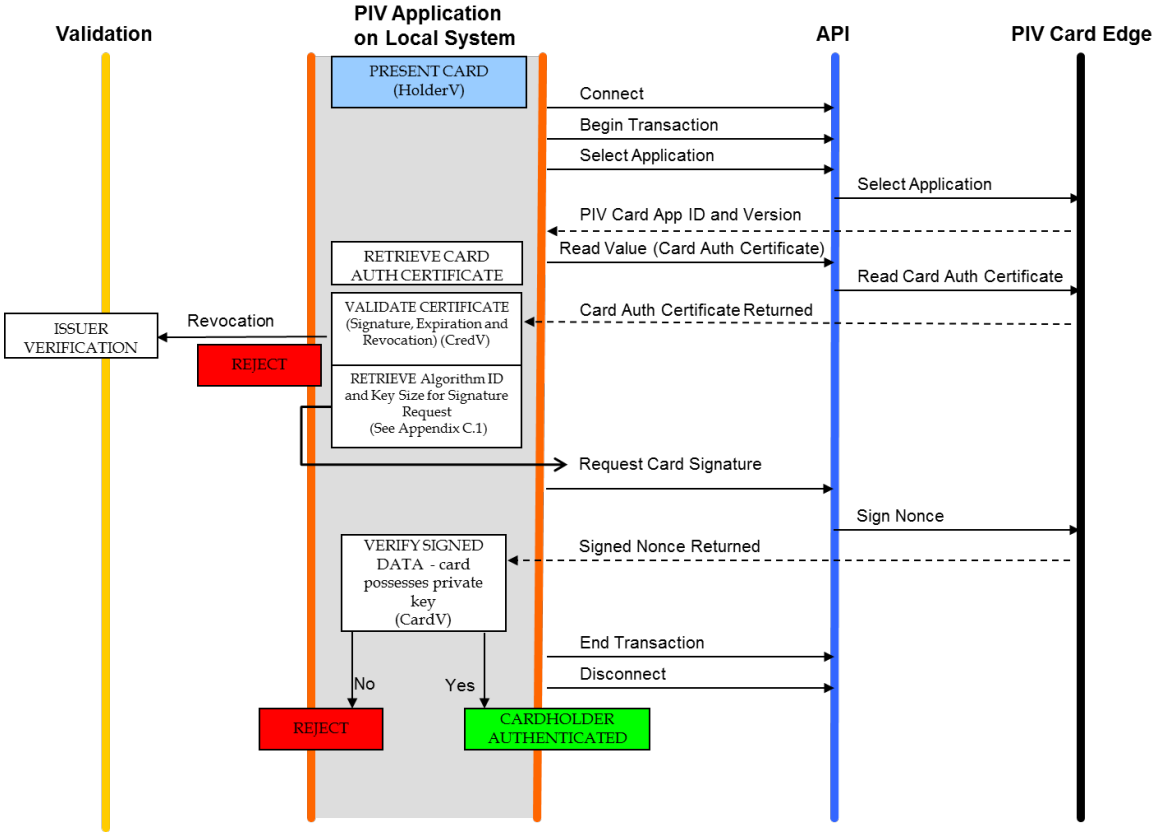

Fig. 4. Authentication using an asymmetric Card Authentication Key

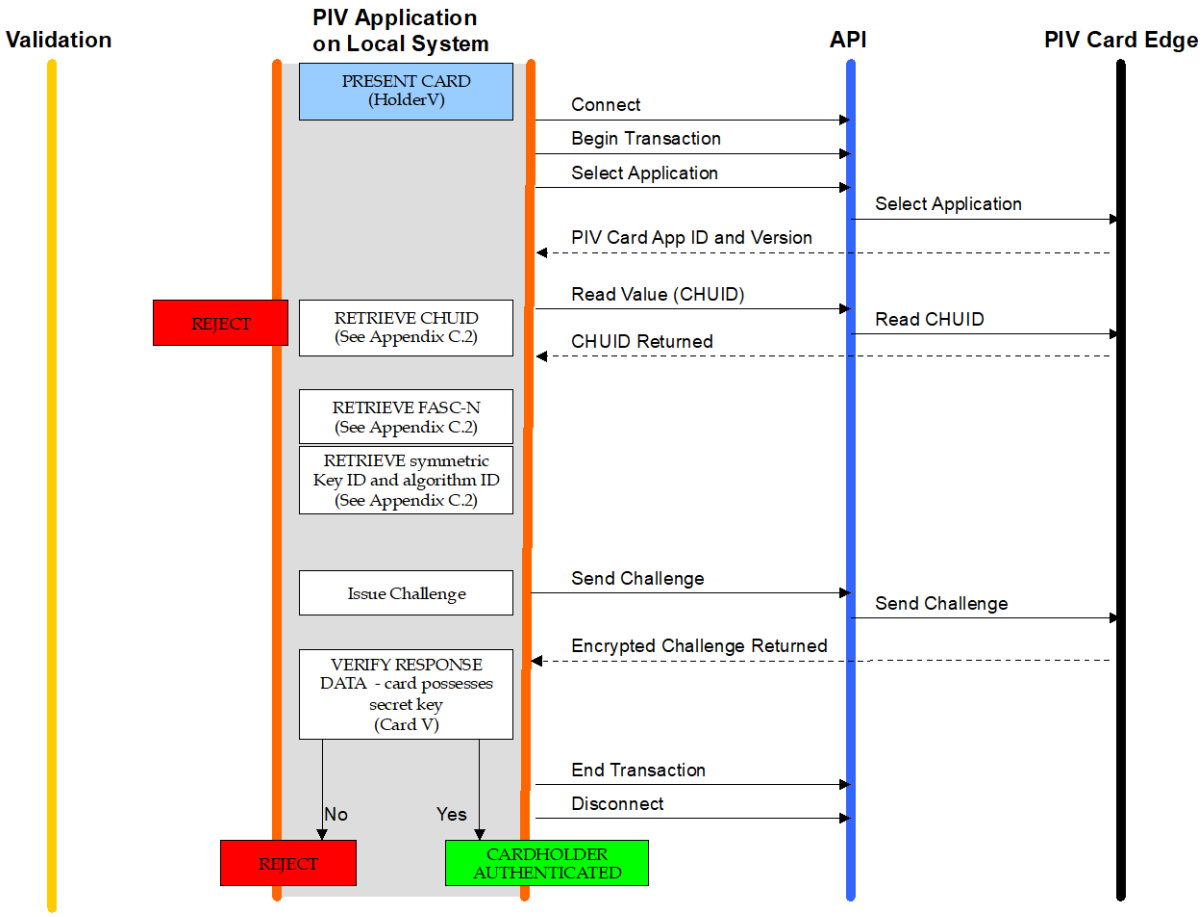

Fig. 5. Authentication using a symmetric Card Authentication Key (DEPRECATED)

B.1.4. Authentication Using OCC (OCC-AUTH)

The OCC-AUTH authentication mechanism is implemented by performing OCC over secure messaging. The PIV Application authenticates the PIV Card as part of the process of establishing secure messaging. When the live-scan fingerprint 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 SP 800-73-5 Part 2 and then performing the VERIFY command, as illustrated in **Fig. 6**.

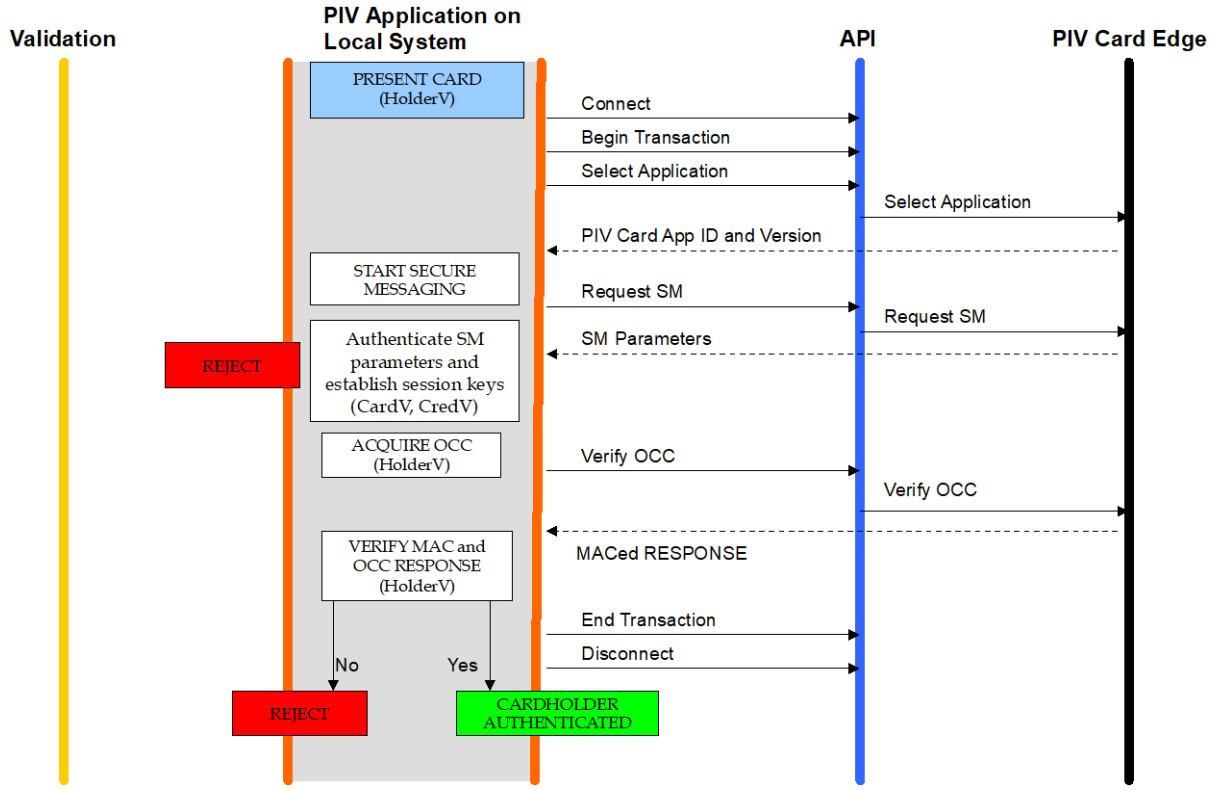

Fig. 6. Authentication using OCC

B.1.5. Authentication Using PIV Visual Credentials (Deprecated)

Figure 7 shows the deprecated authentication mechanism in which a human guard authenticates the cardholder using the visual credentials held by the PIV Card. The authentication mechanism has been deprecated in FIPS 201-3 and MAY be removed from a future edition of the standard.

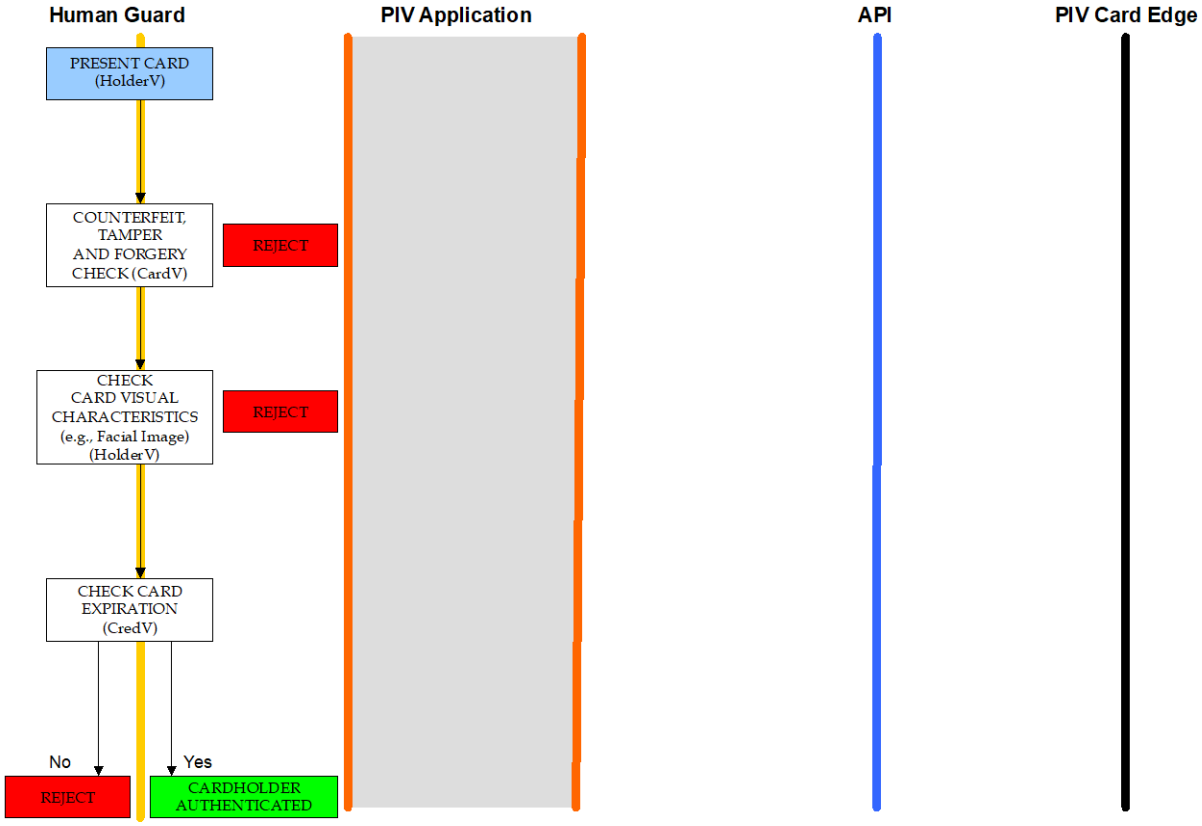

Fig. 7. Authentication using PIV Visual Credentials (DEPRECATED)

B.1.6. Authentication Using PIV CHUID (Removed)

The content of this section has been removed since the CHUID as an authentication mechanism is no longer allowed under FIPS-201. However, the CHUID data element itself remains on-card to support other authentication mechanisms. For example, the BIO and BIO-A authentication mechanisms use the CHUID data element as a source for the card's expiration date. The CHUID data element also provides the content signing certificate for these authentication mechanisms as well as unique identifiers for PACS ACLs.

B.1.7. Authentication Using Secure Messaging Key (SM-AUTH)

If the PIV Card supports the secure messaging protocol, then the secure messaging key, corresponding CVC, and key establishment protocol (see Section 4 of SP 800-73-5 Part 2) CAN be used for authentication of the PIV Card and the cardholder (SM-AUTH). The secure messaging protocol authenticates the PIV Card via the secure messaging key. Any established session keys SHALL be zeroized after authentication if bits b3 and b4 of subsequent command CLA bytes are set to zero.

Figure 8 shows the authentication mechanism using the secure messaging key.

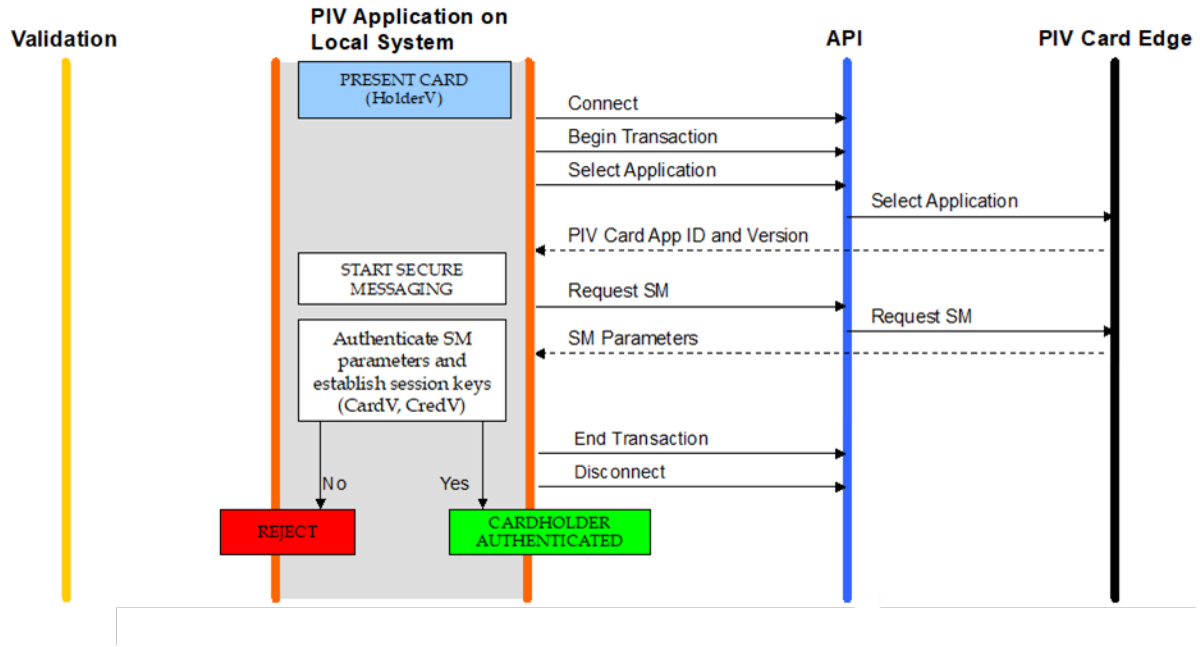

Fig. 8. Authentication using the secure messaging key

B.2. Summary Table

Table 45 summarizes the types of validation activities that are included in each of the PIV authentication mechanisms described earlier in this section.

Table 45. Summary of PIV authentication mechanisms

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
Secure Messaging Key	Perform key agreement to establish session keys	Certificate validation of a Secure Messaging Card Verifiable Certificate	Possession of Card
Symmetric Card Authentication Key (Deprecated)	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 (Deprecated)	Counterfeit, tamper, and forgery check	Expiration check	Possession of Card Match of card visual characteristics with cardholder

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.[34] For example, a relying party performing the authentication mechanism described in Appendix B.1.2 CAN expect to perform a challenge and response cryptographic authentication with a 3072-bit or a 2048-bit RSA key or an ECDSA (Curve P-256 or Curve P-384) key.

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

C.1. PIV Algorithm Identifier Discovery for Asymmetric Cryptographic Authentication

As illustrated in the authentication 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. In contrast, the PIV algorithm identifier 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. Prior to issuing the challenge command, the relying party retrieved and parsed the X.509 certificate from the card to validate the certificate and extract the public key for the pending verification of the signed nonce once returned from the card. The PIV algorithm identifier CAN be identified during the parsing of the X.509 certificate in two steps:[35]

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 4 of SP 800-78.

Step 2: Key Size Discovery

If the algorithm type 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 or P-384 for all elliptic curve PIV Authentication keys and Card Authentication keys.

If the algorithm type 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.

[34] Table 1 of SP 800-78 lists the various algorithms and key sizes that may be used for each PIV Key Type.
[35] 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 9 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 that resides on 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 extract either the Card UUID or the Agency Code || System code || Credential Number from the CHUID's FASC-N.
- 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 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.

Appendix D. List of Symbols, Abbreviations, and 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 Standard

FISMA
Federal Information Security Management Act

GSC-IS
Government Smart Card Interoperability Specification

GUID
Global Unique Identification number

HSPD
Homeland Security Presidential Directive

ICC
Integrated Circuit Card

IEC
International Electrotechnical Commission

INCITS
InterNational Committee for Information Technology Standards

ISO
International Organization for Standardization

ITL
Information Technology Laboratory

LSB
Least Significant Bit

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

URL
Uniform Resource Locator

UUID
Universally Unique Identifier

VCI
Virtual Contact Interface

Appendix E. Glossary

algorithm identifier
A 1-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. [ISO7816, Part 4, adapted]

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 8824-2:2021

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 certification authority, and the information needed to verify the certificate.

data object
An item of information seen at the card command interface with a specified a name, a description of logical content, a format, and a coding.

key reference
A 1-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
A deprecated (previously 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. [ISO8824, adapted]

pairing 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.

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.

Appendix F. Notation

The 16 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, such as '2D'. The two hexadecimal digits are represented in quotations '2D' or as 0x2D. A sequence of bytes MAY be enclosed in single quotation marks (e.g., 'A0 00 00 01 16') rather than given as a sequence of individual bytes (e.g., '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 a 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 that the data object SHALL appear in the template. Optional means that the data object MAY appear in the template. For conditional data objects, the conditions under which they are required are provided.

In other tables, the M/O/C column identifies the 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.

This document uses the following typographical conventions in text:

- Specific terms in **CAPITALS** represent normative requirements. When these same terms are not in **CAPITALS**, the term does not represent a normative requirement.
- The terms **SHALL** and **SHALL NOT** indicate requirements to be strictly followed in order to conform to the publication and from which no deviation is permitted.
- The terms **SHOULD** and **SHOULD NOT** indicate that among several possibilities, one is recommended as particularly suitable without mentioning or excluding others, that a certain course of action is preferred but not necessarily required, or that — in the negative form — a certain possibility or course of action is discouraged but not prohibited.
- The terms **MAY** and **NEED NOT** indicate a course of action that is permissible within the limits of the publication.
- The terms **CAN** and **CANNOT** indicate a material, physical, or causal possibility or capability or — in the negative — the absence of that possibility or capability.

Appendix G. 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 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 (SP 800-73-5 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)

Version	Release Date	Updates
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 (SP 800-73-5 Part 2, Section 3.2.4) • Added UUID feature for non-Federal issuer cards (Part 1, Section 3.3) • Expanded SP 800-73-5 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 SP 800-73-5 Part 3

Version	Release Date	Updates
SP 800-73-4	April 2015	• 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 and 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 a 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 SP 800-73-5 Part 3 • Expanded Part 1, Appendix C (PIV Algorithm Identifier Discovery) to include an Algorithm Identifier discovery for Secure Messaging • Expanded SP 800-73-5 Part 2, Appendix A (GENERAL AUTHENTICATE examples) to illustrate use of VCI

Version	Release Date	Updates
SP 800-73-4	Feb 8, 2016 (Errata update)	• Relaxed interface requirements to allow RESET RETRY COUNTER, PUT DATA, and GENERATE ASYMMETRIC KEY PAIR to be performed over the contactless interface if they are used for card management operations • Allowed use of VERIFY command with key references other than '00', '80', '96', '97', and '98' if they are used for card management operations • Removed the requirement for the PIV Card Application to return a specific error status word ('6A 81' or '69 82') if the interface requirements for submitting the VERIFY command (e.g., contact, secure messaging, virtual contact) are not satisfied • Allowed use of CHANGE REFERENCE DATA command with key references other than '80' and '81' if they are used for card management operations • Removed the requirement for the PIV Card Application to return a specific error status word ('6A 81' or '69 82') if the interface requirements for submitting the CHANGE REFERENCE DATA command (e.g., contact, virtual contact) are not satisfied • Allowed use of RESET RETRY DATA command with key references other than '80' if they are used for card management operations • Updated PIV Card Application Authentication Data References table with number of allowed retries for primary and secondary fingers for OCC and PIV Card Application PIN

Version	Release Date	Updates
SP 800-73-5	INSERT DATE	• Removed the previously deprecated Extended Application CardURL and Security Object Buffer elements from the Card Capability Container data object • Removed the previously deprecated Buffer Length, DUNS, and Organizational Identifier elements from the CHUID data object • Removed the previously deprecated MSCUID element from all X.509v3 Certificate data objects other than certificates for retired key management keys • Deprecated SYM-CAK and VIS authentication mechanisms • Removed previously deprecated CHUID authentication mechanism • Added SM-AUTH as a single-factor additional authentication mechanism • Deprecated use of separate content signing keys for biometric data and CHUID • Restricted the number of consecutive activation retries for each of the activation methods (i.e., PIN and OCC attempts) to be 10 or less • Marked SP 800-73-5 Part 3 as optional • Added the use of the facial image biometric for automated facial comparison (i.e., not just for issuance processes) through BIO and BIO-A authentication mechanisms • Enabled OCC reset through CHANGE REFERENCE DATA command in SP 800-73-5 Part 2 • Updated allowed cryptographic algorithms to match SP 800-78-5 • Specified that fingerprints used for OCC MAY be taken from the full set of fingerprints collected for PIV background investigations and SHOULD be imaged from fingers not imaged for off-card one-to-one comparison • Updated the container minimum capacity for many of PIV Data Containers • Deleted the details of incompatibilities between versions of this document from the Configuration Management section • Clarified that the Card UUID, Expiration Date, and Cardholder UUID fields cannot be modified post-issuance • Clarified that NPIVP conformance testing will no longer be performed for PIV Middleware • Moved set of errata changes in SP 800-73-4 into the Revision History • Leveraged the latest NIST publication template, including introductory pages, content, and styles

1539