Module 6/G: FIPS 201, PIV Card and Federal Identity Management

Smart Card Alliance
Certified Smart Card Industry Professional/Government
Accreditation Program

About the Smart Card Alliance

The Smart Card Alliance is a not-for-profit, multi-industry association working to stimulate the understanding, adoption, use and widespread application of smart card technology. Through specific projects such as education programs, market research, advocacy, industry relations and open forums, the Alliance keeps its members connected to industry leaders and innovative thought. The Alliance is the single industry voice for smart cards, leading industry discussion on the impact and value of smart cards in the U.S. and Latin America. For more information please visit http://www.smartcardalliance.org.

Important note: *The CSCIP training modules are only available to LEAP members who have applied and paid for CSCIP certification. The modules are for CSCIP applicants ONLY for use in preparing for the CSCIP exam. These documents may be downloaded and printed by the CSCIP applicant. Further reproduction or distribution of these modules in any form is forbidden.*

Table of Contents

TABLE OF CONTENTS **3**

1 INTRODUCTION **7**

2 OVERVIEW **8**

2.1 HSPD-12 8
2.2 FIPS 201 8
2.3 FIPS 201 BEYOND THE U.S. FEDERAL GOVERNMENT 9
2.4 TECHNICAL SPECIFICATIONS SUPPORTING FIPS 201-2 10
2.5 PRINCIPAL CHANGES BETWEEN FIPS 201-1 AND FIPS 201-2 10

3 FIPS 201, PART 1: COMMON IDENTITY, SECURITY AND PRIVACY REQUIREMENTS **12**

3.1 CONTROL OBJECTIVES 12
3.2 PIV IDENTITY PROOFING AND REGISTRATION REQUIREMENTS 12
3.3 CREDENTIALING REQUIREMENTS 14
3.4 BIOMETRIC DATA COLLECTION FOR BACKGROUND INVESTIGATIONS 14
3.5 BIOMETRIC DATA COLLECTION FOR PIV CARD 14
3.6 BIOMETRIC DATA USE 14
3.7 CHAIN-OF-TRUST 15
3.8 PIV CARD ISSUANCE REQUIREMENTS 15
3.8.1 Special Rule for Pseudonyms 16
3.8.2 Grace Period 16
3.8.3 PIV Card Maintenance Requirements 16
3.8.4 PIV Card Reissuance Requirements 16
3.8.5 Special Rule for Name Change by Cardholder 17
3.8.6 PIV Card Post Issuance Update Requirements 17
3.8.7 PIV Card Verification Data Reset 17
3.8.8 PIV Card Termination Requirements 17
3.9 DERIVED PIV CREDENTIALS ISSUANCE REQUIREMENTS 17
3.10 PIV PRIVACY REQUIREMENTS 17

4 PIV SYSTEM OVERVIEW **19**

4.1 FUNCTIONAL COMPONENTS 19
4.1.1 PIV Front-End System 20
4.1.2 PIV Card Issuance and Management Subsystem 21
4.1.3 PIV Relying Subsystem 21
4.2 PIV CARD LIFECYCLE ACTIVITIES 21

5 PIV FRONT-END SUBSYSTEM **24**

5.1 PIV CARD PHYSICAL CHARACTERISTICS 24
5.1.1 Printed Material 24
5.1.2 Tamper Proofing and Resistance 24
5.1.3 Physical Characteristics and Durability 25
5.2 VISUAL CARD TOPOGRAPHY 26
5.3 PIV CARD LOGICAL CHARACTERISTIC 28
5.4 PIV CARD ACTIVATION 29
5.4.1 Activation by Cardholder 29
5.4.2 Activation by Card Management System 30
5.5 PIV DATA MODEL ELEMENTS 30
5.5.1 Mandatory Data Elements 31

5.5.2 Conditional Data Elements 33
5.5.3 Optional Data Elements 33
5.5.4 Inclusion of Universally Unique IDentifiers (UUIDs) 35
5.5.5 Data Object Containers and associated Access Rules and Interface Modes 35
5.6 CRYPTOGRAPHIC SPECIFICATIONS 36
5.6.1 Secure Messaging and Virtual Card Interface 38
5.7 BIOMETRIC DATA 40
5.7.1 Biometric Data Access 40
5.7.2 On-Card Biometric Comparison (OCC) 40
5.8 CARD READER SPECIFICATIONS 41
5.8.1 Contact Reader Specifications 41
5.8.2 Contactless Reader Specifications 41
5.8.3 Reader Resilience and Flexibility 41
5.8.4 Card Activation Device Requirements 41

6 PIV CARD ISSUANCE AND LIFECYCLE 43

6.1 CREATING A NEW PIV RECORD AND ISSUING A NEW PIV CARD 45
6.1.1 Sponsorship 45
6.1.2 Enrollment 45
6.1.3 Adjudication 46
6.1.4 Issuance 47
6.2 MAINTAINING AN EXISTING PIV RECORD AND CARD 47
6.3 MANAGING PIV KEYS 51

7 FIPS 201 AND BIOMETRICS 53

7.1 BIOMETRIC DATA COLLECTION, STORAGE, AND USAGE 53
7.2 ALTERNATIVE BIOMETRIC USAGE 54

8 AUTHENTICATION LEVELS 56

8.1 OMB M-04-04 56
8.2 SP 800-63 58
8.3 AUTHENTICATION LEVELS, FIPS 201 AND PIV 61
8.3.1 FIPS 201 Assurance Levels 61
8.3.2 PIV Authentication Mechanisms 62

9 FIPS 201/PIV CARD USE CASES: PHYSICAL ACCESS 65

9.1 CURRENT PACS 65
9.2 FICAM ROADMAP: TARGET PIV CARD USE WITH PACS 66
9.2.1 Smart Card Authentication Mechanisms 67
9.3 SELECTION OF AUTHENTICATION MECHANISMS 69
9.4 ALTERNATIVE AUTHENTICATION MECHANISMS USING THE PIV CARD 70
9.4.1 Operational Biometrics with Enrollment on System and Match on System 70
9.4.2 Reference Biometric with Match on System and Contactless Read of Encrypted Biometric Template on Card 71
9.4.3 Operational Biometric with Enrollment on Card and Match on Card 71
9.4.4 PIN-to-PACS as Single Factor Knowledge 72
9.4.5 PIN-to-Card 72
9.4.6 Card with PIN-to-PACS 73
9.5 PACS PROVISIONING 74
9.6 PACS MIGRATION 75
9.6.1 Current PACS Architecture 76
9.6.2 PACS and the Introduction of PIV and PIV-I Cards 76

9.6.3 Target PACS Architecture 78

10 FIPS 201/PIV CARD USE CASES: LOGICAL ACCESS 80

10.1 PIV CARD AUTHENTICATION MECHANISMS FOR LOGICAL ACCESS 80
10.2 USE OF THE PIV CARD FOR LOGICAL ACCESS APPLICATIONS 81
10.2.1 PKI Credentials 81
10.2.2 Password Tokens for Logon 82
10.2.3 Logical Access to Networks, Systems, Applications and Data 82
10.2.4 Secure Document or Communication with PKI 84
10.2.5 Other Uses of the PIV Card for Logical Access Applications 84

11 FIPS 201/PIV CARD AND SERVICES CERTIFICATION, TESTING AND PRODUCT ACQUISITION 86

11.1 NIST PERSONAL IDENTITY VERIFICATION PROGRAM (NPIVP) 86
11.2 FIPS 140-2 86
11.3 FIPS 201 EVALUATION PROGRAM 87
11.4 GSA APPROVED PRODUCT LIST 88
11.5 PIV CARD INFRASTRUCTURE AND ISSUANCE 88

12 PIV-I: INTEROPERABILITY BEYOND THE FEDERAL GOVERNMENT 90

12.1 PIV INTEROPERABILITY FOR NON-FEDERAL ISSUERS (NFI) 90
12.2 MINIMUM NFI CARD REQUIREMENTS 91
12.2.1 Common Terminology for Identity Cards 91
12.2.2 Assumptions 92
12.2.3 Requirements for NFI Cards 92
12.2.4 Technical Requirements for NFI Cards 92
12.2.5 Identifier Namespace 93
12.2.6 Trusted Identity 94

13 FEDERAL PKI, PIV AND PIV-I 97

13.1 FEDERAL PKI TIMELINE 97
13.2 THE FEDERAL PKI LANDSCAPE 99
13.2.1 The Federal Public Key Infrastructure (FPKI) 99
13.2.2 Legacy FPKI Participants 102
13.2.3 External FPKI Partners 102
13.2.4 SSP PKI "Clones" 103
13.2.5 Partnership with Academia 104
13.2.6 The Four Bridges Forum 104
13.3 THE VALUE OF PKI TO THE FEDERAL GOVERNMENT 104
13.3.1 Qualitative Benefits of PKI 104
13.3.2 Quantitative Benefits of PKI 106
13.3.3 Case Studies 109
13.4 THE FUTURE OF PKI – PIV, PIV-I AND INDUSTRY DIRECTIONS 110

14 FEDERAL IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT GUIDELINES 112

14.1 OVERVIEW OF IDENTITY, CREDENTIAL AND ACCESS MANAGEMENT 113
14.1.1 ICAM in the Federal Government 113
14.1.2 Identity Management 113
14.1.3 Credential Management 114
14.1.4 Access Management 115
14.1.5 ICAM Intersection 115
14.2 ICAM GOVERNANCE 115

14.3 ICAM SEGMENT ARCHITECTURE 116
14.3.1 Performance Architecture 117
14.3.2 Business Architecture 118
14.3.3 Data Architecture 119
14.3.4 Service Architecture 119
14.3.5 Technical Architecture 120
14.4 SUMMARY 121

15 OTHER U.S. GOVERNMENT SMART CARD IMPLEMENTATIONS 122

15.1 DEPARTMENT OF DEFENSE COMMON ACCESS CARD 122
15.1.1 DoD Identity Management 122
15.2 TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL 123
15.3 FIRST RESPONDER AUTHENTICATION CREDENTIAL 125
15.3.1 PIV-I/FRAC Technology Transition Working Group 126
15.3.2 Commonwealth of Virginia First Responder Authentication Credentials 128

16 STANDARDS, POLICY GUIDANCE AND REFERENCES 129

16.1 STANDARDS 129
16.2 POLICY DOCUMENTS 131
16.3 OTHER REFERENCES 132

17 ANNEXES 134

17.1 HSPD -12 CREDENTIALS IN USE AS OF DECEMBER 1, 2013 134
17.2 SECURE MESSAGING FUNDAMENTALS 135
17.3 TRADITIONAL IMPLEMENTATION EXAMPLES OF SECURE MESSAGING 135
17.3.1 Electronic Passport / International Driver's License 135
17.3.2 GlobalPlatform Secure Channel Protocol (SCP) 136
17.3.3 PIV and Secure Messaging 138

18 ACKNOWLEDGEMENTS 140

1 Introduction

This module is part of the Smart Card Alliance CSCIP/Government certification. The module focuses on the U.S. government's implementation of the Federal identity management infrastructure and smart card-based employee and contractor identity credentials that resulted from Homeland Security Presidential Directive 12 (HSPD-12). After reviewing this module, CSCIP applicants should be able to answer the following questions and be familiar with examples of reference smart card implementations.

- What are HSPD-12, FIPS 201 and the PIV card?
- What are FIPS 201 identity and security requirements?
- What are the physical and logical characteristics of the PIV card?
- What are the PIV Card data model and its options?
- How are PIV Card PKI certificates and biometrics used?
- What are key requirements and processes for issuing and maintaining PIV cards?
- How are biometrics used with FIPS 201 processes?
- How are PIV cards used with physical and logical access control systems?
- What are PIV interoperable and PIV compatible cards and how do they differ from PIV cards?
- What are Federally-defined identity levels of assurance and what authentication mechanisms are enabled with PIV cards?
- How are FIPS 201 products evaluated and certified?
- What are key standards and specifications that govern the implementation of FIPS 201?
- What are the components of the federal PKI infrastructure and how does the infrastructure enable interoperability among federal agencies, with state and local governments and with business partners?
- What is the Federal Identity, Credential and Access Management architecture and how will it affect implementations going forward?
- What other NIST publications are related to FIPS 201-2 (e.g., SP 800-73, 76, 78, 79, 87,96, 156, 157?)

This module does not include a general description of smart card technology, applications and security or the general use of smart cards in identity and security applications.

CSCIP applicants should also review:

- Module 1 – Smart Card Fundamentals;
- Module 2 – Security;
- Module 3 – Smart Card Application and Data Management; and
- Module 5 – Smart Card Usage Models – Identity and Security.

2 Overview

2.1 HSPD-12

Homeland Security Presidential Directive 12 (HSPD-12)[1], issued on August 27, 2004, mandated the need "to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification." HSPD-12 specifically calls for the use of a common identification credential for "gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems."

HSPD-12 requires that the Federal credential be secure and reliable, which is defined as a credential that:

- Is issued based on sound criteria for verifying an individual's identity;
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;
- Can be rapidly authenticated electronically; and
- Is issued only by providers whose reliability has been established by an official accreditation process.

The Department of Commerce and National Institute of Standards and Technology (NIST) were tasked with producing a standard for secure and reliable forms of identification. In response, NIST published Federal Information Processing Standard Publication 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, on February 25, 2005. This document was updated based on the new version FIPS 201-2 which was published in August 2013. The FIPS 201 PIV Card is to be used for both physical and logical access control, and other applications as determined by the individual agencies. NIST has also produced a number of special publications that expand on the FIP 201 and PIV standards.[2]

2.2 FIPS 201

FIPS 201 defines the identity vetting, enrollment, and issuance requirements for a common identity credential and the technical specifications for an interoperable government employee and contractor ID card—the PIV card. The FIPS 201 PIV Card is a smart card with both contact and contactless interfaces that is now being issued to all Federal employees and contractors.

FIPS 201 consists of two parts: Part 1, PIV I[3] (Policy) and Part 2, PIV II (Technology). The standards in PIV I support the control objectives and security requirements described in HSPD-12, including the personal identity proofing, registration and issuance processes. The standards in PIV II support the technical interoperability requirements described in HSPD-12. PIV II also specifies standards for implementing identity credentials on integrated circuit cards (i.e., smart cards) for use in a Federal PIV system.

The FIPS 201 standard defines authentication mechanisms offering varying degrees of security. Federal departments and agencies will determine the level of security and authentication mechanisms appropriate for their applications. The standard does not specify access control policies or requirements for Federal departments and agencies. Therefore, the scope of FIPS 201 is limited to authentication of an individual's identity. Authorization and access control are outside the scope of FIPS 201.[4]

---

1 "Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004, http://www.idmanagement.gov/homeland-security-presidential-directive-12

2 All NIST publications can be found on the NIST PIV Program web site, http://csrc.nist.gov/groups/SNS/piv/ .

3 The term PIV I (which stands for FIPS 201-2 policies) must not be confused with PIV-I which stands for PIV-Interoperable and is used for cards issued by non Federal issuers. See Section 2.3 in this document)

4 Federal Information Processing Standard Publication 201 (FIPS 201-2), "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013, *Section 1.2* p.2

As of December 1st, 2013, about 4.5 million HSPD-12 credentials have been issued to Federal employees (96% of the total population) and close to 1 million credentials have been issued to contractors.[5] Twenty federal credential issuance infrastructures are in operation nationwide.

A growing number of approved vendors of logical and physical access systems and applications have developed products built on FIPS 201 and industry standards for smart cards. FIPS 201 has attracted international attention and is under consideration for government, public safety, and critical infrastructure personnel in other countries.

2.3 FIPS 201 beyond the U.S. Federal Government[6]

While only Federal agencies can issue "official" PIV cards, other organizations can follow FIPS 201 processes, use FIPS 201-defined technologies, and implement credentials that are *PIV interoperable* or follow the *CIV (Commercial Identity Verification)* definition[7], as appropriate.

As a result of non-federal issuers (NFIs) of identity cards expressing a desire to produce identity cards that can technically interoperate with Federal government PIV systems and that can be trusted by Federal government relying parties, the Federal CIO Council published the guidance document, *Personal Identity Verification Interoperability for Non-Federal Issuers,* in July 2010. Additional detail about PIV interoperable and commercial compatible cards can be found in Section 12.

A PIV interoperable credential is a credential that meets the FIPS 201 technical standards (and can therefore work with PIV infrastructure elements, such as card readers) and also follows the FIPS 201 process for issuing credentials but without the same background verification on the card holder. Following the FIPS 201 process for credential issuance allows all Federal relying parties to trust the identity represented by the card, across organizations. This trust is established by a common enrollment, registration, and issuance process and a strong authentication credential that leverages a cross-certified and federated public key infrastructure. A PIV interoperable credential would be of great value to organizations that do business with the government and have a requirement to issue interoperable identity credentials. In addition, related organizations within an industry could decide to follow common FIPS 201 processes to establish a basis for trusting identity credentials across organizations.

A CIV credential is a one that meets the FIPS 201 technical specifications but may not follow the FIPS 201 process for credential issuance or cardholder identity verification. Federal relying parties cannot automatically trust the card. Organizations issuing compatible credentials can benefit by being able to use the growing range of products on the GSA FIPS 201 Evaluation Program Approved Products List. Cards, readers, software, and other products can be purchased from a variety of vendors, be connected, and function as a system.

Organizations can choose to implement interoperable or compatible credentials. FIPS 201 provides a defined framework and technical specifications for organizations to follow for both. By basing identity credentialing efforts on FIPS 201, organizations can:

- Follow a proven process for identity vetting
- Implement an identity vetting process that provides the basis for trusting identities across organizations or with Federal agencies
- Implement an identity credentialing solution that has the potential to be interoperable and compatible across organizations or with Federal agencies

---

[5] http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/hspd-12_reporting_workbook_status_report_q1fy2014.pdf

[6] Sources: "Using FIPS 201 and the PIV Card for the Corporate Enterprise," Smart Card Alliance white paper, October 2008, http://www.smartcardalliance.org/pages/publications-piv-corporate-enterprise ; "Personal Identity Verification Interoperability for Non-Federal Issuers," CIO Council, July 2010, http://www.idmanagement.gov/sites/default/files/documents/PIV_IO_NonFed_Issuers.pdf

[7] http://www.smartcardalliance.org/resources/pdf/CIV_WP_101611.pdf

- Acquire proven products and services from multiple vendors that meet FIPS 201 technical specifications

2.4 Technical Specifications Supporting FIPS 201-2

Reference documents which previous versions were already supporting FIPS 201-1[8] are:

- SP 800-73-4 – Interfaces for PIV
- SP 800-76 – Biometric Specifications for PIV

Reference documents that were added in FIPS 201-2 are:

- SP 800-78 – Cryptographic Algorithms and Key Sizes for PIV
- SP 800-79 – Guidelines for the Accreditation of PIV Card Issuers
- SP 800-87 – Codes for the Identification of Federal & Federally-Assisted Organizations
- SP 800-96 – PIV Card to Reader Interoperability Guidelines
- SP 800-156 – Representation of PIV Chain of Trust Import & Export[9]
- SP 800-157 – Guidelines for Derived PIV Credentials

Other technical documents related to FIPS 201-2 but not mentioned explicitly in FIPS 201-2 include the following:

Test guidelines documents are:

- SP 800-85A – PIV Card Application & Middleware Interface Test Guidelines
- SP 800-85B – PIV Data Model Test Guidelines
- SP 800-166 – PIV Derived Credential Test Requirements

Documents created for FIPS 201-1 which are not revised or confirmed yet for FIPS 201-2 are:

- SP 800-116 – A Recommendation for the Use of PIV Credentials in PACS. This document is to be considered along with the E-PACS paper issued by the Federal CIO Council on the subject: Personal Identity Verification (PIV) in Enterprise Physical Access Control Systems (E-PACS)

Documents defined (or used) for FIPS 201-1 and not relevant anymore (deprecated) are:

- SP 800-104 - PIV Visual Topography – June 29, 2007. PIV Card topography and all its options are now in the FIPS 201-2 document itself.

2.5 Principal changes between FIPS 201-1 and FIPS 201-2

The principal changes between FIPS 201-1 and FIPS 201-2 are the following:

- Modified the requirement for accreditation of PIV card issuer to include an independent review.
- Incorporated references to credentialing guidance and requirements issued by the Office of Personnel Management (OPM) and Office of Management and Budget (OMB).
- Made the facial image data element on the PIV card mandatory.
- Added the option to collect and store iris biometric data on the PIV card.
- Added option to use electronic facial image for authentication in operator-attended environments.
- Incorporated the content from Form I-9 that is relevant to FIPS 201.
- Introduced the concept of a “chain-of-trust” optionally maintained by a PIV card issuer.
- Changed the maximum life of PIV card from 5 years to 6 years.
- Added requirements for issuing a PIV card to an individual under a pseudonymous identity.
- Added requirements for issuing a PIV card to an individual within grace period.
- Added requirements for post-issuance updates.

[8] For a complete list of NIST SP 800 publications, see: http://csrc.nist.gov/publications/PubsSPs.html
[9] As of February 2015, this document is referenced in FIPS 201-2 but has not been published by NIST yet.

- Added option to allow for remote PIN resets.
- Introduced the ability to issue derived PIV credentials.
- Made the employee affiliation color-coding and the large expiration date in the upper right-hand corner of the card mandatory.
- Made all four asymmetric keys and certificates mandatory.[10]
- Introduced the concept of a virtual contact interface over which all functionality of the PIV card is accessible.
- Added the possibility of using secure messaging (over contact and contactless) with key confirmation.
- Added PIN minimal length (6 numeric minimum) enforcement by the PIV card.
- Added a mandatory UUID as a unique identifier for the PIV card in addition to the FASC-N.
- Added optional on-card biometric comparison as a means of performing card activation and as a PIV authentication mechanism.
- Removed direct requirement to distribute certificates and CRLs via LDAP.
- Updated authentication mechanisms to enable variations in implementations.
- Require signature verification and certification path validation in the CHUID, BIO, and BIO-A authentication mechanisms.
- The VIS and CHUID authentication mechanisms have been downgraded to indicate that they provide LITTLE or NO assurance on the identity of the cardholder.
- Deprecated the use of the CHUID authentication mechanism.
- Continued with mandatory CHUID data element (it has not been deprecated).

[10] If the cardholder has a government email account at time of issuance; else only the authentication certificates are mandatory.

3 FIPS 201, Part 1: Common Identity, Security and Privacy Requirements

Note: The following sections were extracted from the NIST publication, Federal Information Processing Standard Publication 201 (FIPS 201-2), Personal Identity Verification (PIV) of Federal Employees and Contractors, Part 1, August 2013.

3.1 Control Objectives

[HSPD-12] established control objectives for secure and reliable identification of Federal employees and contractors. These control objectives, provided in paragraph 3 of the directive, are quoted here:

> (3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process.

Each agency's PIV implementation shall meet the four control objectives (a) through (d) listed above such that—

- Credentials are issued
    1. To individuals whose identity has been verified, and
    2. After a proper authority has authorized issuance of the credential.
- A credential is issued only after National Agency Check with Written Inquiries (NACI) (or equivalent or higher) or Tier 1 or higher federal background investigation is initiated, and the Federal Bureau of Investigation (FBI) National Criminal History Check (NCHC) portion of the background investigation is completed.
- An individual is issued a credential only after presenting two identity source documents, at least one of which is a Federal or State government issued picture ID.
- Fraudulent identity source documents are not accepted as genuine and unaltered.
- A person suspected or known to the government as being a terrorist is not issued a credential.
- No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued.
- No credential is issued unless requested by proper authority.
- A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.
- A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential.
- An issued credential is not duplicated or forged, and is not modified by an unauthorized entity.

3.2 PIV Identity Proofing and Registration Requirements

Departments and agencies shall follow an identity proofing and registration process that meets the requirements defined below when issuing PIV cards.

- The organization shall adopt and use an identity proofing and registration process that is approved in accordance with [SP 800-79].

- Biometrics shall be captured as specified in Sections 2.3 and 2.4 of FIPS 201-2.
- The process shall begin by locating and referencing a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record. In the absence of a record, the process shall ensure:
    1. The initiation of a Tier 1 or higher federal background investigation and
    2. The completion of the National Agency Check (NAC)[11] of the background investigation. In cases where the NAC results are not received within 5 days of the NAC initiation, the FBI NCHC (fingerprint check) portion of the NAC shall be complete before PIV card issuance.
- The applicant shall appear in-person at least once before the issuance of a PIV card.
- During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form[12].The identity source documents shall be bound to that applicant and shall be neither expired nor cancelled. If the two identity source documents bear different names, evidence of a formal name change shall be provided. The primary identity source document shall be one of the following forms of identification:
    - A U.S. Passport or a U.S. Passport Card;
    - A Permanent Resident Card or an Alien Registration Receipt Card (Form I-551);
    - A foreign passport;
    - An Employment Authorization Document that contains a photograph (Form I-766);
    - A driver's license or an ID card issued by a state or possession of the United States provided it contains a photograph;
    - A U.S. military ID card;
    - A U.S. military dependent's ID card; or
    - A PIV card.

The secondary identity source document may be from the list above, but cannot be of the same type as the primary identity source document. The secondary identity source document may also be one of the following:

- A U.S. Social Security Card issued by the Social Security Administration;
- An original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal;
- An ID card issued by a federal, state, or local government agency or entity, provided it contains a photograph;
- A voter's registration card;
- A U.S. Coast Guard Merchant Mariner Card;
- A Certificate of U.S. Citizenship (Form N-560 or N-561);
- A Certificate of Naturalization (Form N-550 or N-570);
- A U.S. Citizen ID Card (Form I-197);
- An Identification Card for Use of Resident Citizen in the United States (Form I-179);
- A Certification of Birth Abroad or Certification of Report of Birth issued by the Department

[11] The NAC is an automated record check.
[12] FIPS 201-2 does not refer to the I-9 list of documents anymore and defines its own list.

of State (Form FS-545 or Form DS-1350);

- A Temporary Resident Card (Form I-688);
- An Employment Authorization Card (Form I-688A);
- A Reentry Permit (Form I-327);
- A Refugee Travel Document (Form I-571);
- An Employment authorization document issued by Department of Homeland Security (DHS);
- An Employment Authorization Document issued by DHS with photograph (Form I-688B);
- A driver's license issued by a Canadian government entity; or
- A Native American tribal document.

The PIV identity proofing, registration, issuance, and reissuance processes shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV card without the cooperation of another authorized person.

The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head or deputy secretary (or equivalent) of the Federal department or agency.

The requirements for identity proofing and registration also apply to citizens of foreign countries who are working for the Federal government overseas. However, a process for identity proofing and registration must be established using a method approved by the U.S. Department of State's Bureau of Diplomatic Security, except for employees under the command of a U.S. area military commander. These procedures may vary depending on the country.

3.3 Credentialing Requirements

Federal departments and agencies shall use the credentialing guidance issued by the Director of the Office of Personnel Management (OPM) and Office of Management and Budget (OMB).

3.4 Biometric Data Collection for Background Investigations

Fingerprint collection shall conform to the procedural and technical specifications of [SP 800-76].

3.5 Biometric Data Collection for PIV Card

The following biometric data shall be collected from each PIV applicant:

- Two fingerprints, for off-card comparison. These shall be taken either from the full set of fingerprints collected in Section 2.3 of FIPS 201-2, or collected independently.
- An electronic facial image.

The following biometric data may optionally be collected from a PIV applicant:

- One or two iris images.
- Two fingerprints, for on-card comparison. It is recommended that these be different than the fingerprints collected for off-card comparison.

3.6 Biometric Data Use

The full set of fingerprints shall be used for one-to-many identification in the databases of fingerprints maintained by the FBI.

The two mandatory fingerprints shall be used for preparation of templates to be stored on the PIV card as described in Section 4.2.3.1 of FIPS 201-2. The fingerprints provide an interagency-interoperable authentication mechanism through a match-off-card scheme as described in Section 6.2.1 of FIPS 201-2.

The electronic iris images may be stored on the PIV card as described in Section 4.2.3.1 of FIPS 201-2.

The electronic facial image:

- Shall be stored on the PIV card as described in Section 4.2.3.1 of FIPS 201-2;
- Shall be printed on the PIV Card according to Section 4.1.4.1 of FIPS 201-2;
- May be used for generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.6 of FIPS 201-2; and
- May be used for automated facial authentication in operator-attended PIV issuance, reissuance, and verification data reset processes.

3.7 Chain-of-Trust

A card issuer may optionally maintain, for each PIV card issued, a documentary chain-of-trust for the identification data it collects. The chain-of-trust is a sequence of related enrollment data records that are created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records.

It is recommended that the following data be included in the chain-of-trust:

- A log of activities that documents who took the action, what action was taken, when and where the action took place, and what data was collected.
- An enrollment data record that contains the most recent collection of each of the biometric data collected. The enrollment data record describes the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method. The enrollment data record may also document unavailable biometric data or failed attempts to collect biometric data. The enrollment data record may contain historical biometric data.
- The most recent unique identifiers (i.e., Federal Agency Smart Credential Number (FASC-N) and Universally Unique IDentifier (UUID)) issued to the individual. The record may contain historical unique identifiers.
- Information about the authorizing entity who has approved the issuance of a credential.
- Current status of the background investigation, including the results of the investigation once completed.
- The evidence of authorization if the credential is issued under a pseudonym.
- Any data or any subsequent changes in the data about the cardholder. If the changed data is the cardholder's name, then the issuer should include the evidence of a formal name change.

3.8 PIV Card Issuance Requirements

Departments and agencies shall meet the requirements defined below when issuing PIV cards. The issuance process used when issuing PIV cards shall be accredited by the department or agency as satisfying the requirements below and approved in writing by the head or deputy secretary (or equivalent) of the Federal department or agency.

- PIV cards are issued after a proper authority has authorized issuance of the credential.
- The organization shall use an approved PIV credential issuance process in accordance with [SP 800-79].

- Before issuing the PIV card, the process shall ensure that a previously completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation is on record. In the absence of a record, the required federal background investigation shall be initiated. The PIV card should not be issued before the results of the NAC are complete. However, if the results of the NAC have not been received in 5 days, the PIV card may be issued based on the FBI NCHC. In the absence of an FBI NCHC (e.g., due to unclassifiable fingerprints) the NAC results are required prior to issuing a PIV Card. The PIV card shall be terminated if the results of the background investigation so justify.
- Biometrics used to personalize the PIV card must be those captured during the identity proofing and registration process.
- During the issuance process, the issuer shall verify that the individual to whom the PIV card is to be issued is the same as the intended applicant/recipient as approved by the appropriate authority. Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the applicant against biometrics available on the PIV card or in the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the PIV card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide two identity source documents (as specified in FIPS 201-2 Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image printed on the PIV card.
- The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited) in accordance with [SP 800-79].
- The PIV card shall be valid for no more than six years. PIV cards that contain topographical defects (e.g., scratches, poor color, fading, etc.) or that are not properly printed shall be destroyed. The PIV card issuer is responsible for the card stock, its management, and its integrity.

3.8.1 Special Rule for Pseudonyms

In limited circumstances, Federal employees and contractors are permitted to use pseudonyms during the performance of their official duties with the approval of their employing agency.

3.8.2 Grace Period

In some instances an individual's status as a Federal employee or contractor will lapse for a brief time period.

In these instances, the card issuer may issue a new PIV card without repeating the identity proofing and registration process if the issuer has access to the applicant's chain-of-trust record and the applicant can be reconnected to the chain-of-trust record.

3.8.3 PIV Card Maintenance Requirements

The data and credentials held by the PIV card may need to be updated or invalidated prior to the expiration date of the card. The cardholder may change his or her name, retire, or change jobs; or the employment may be terminated, thus requiring invalidation of a previously issued card. In this regard, procedures for PIV card maintenance must be integrated into department and agency procedures to ensure effective card maintenance.

3.8.4 PIV Card Reissuance Requirements

Reissuance is the process by which a new PIV card is issued to a cardholder without the need to repeat the entire identity proofing and registration procedure. The reissuance process may be used to replace a

PIV card that is nearing expiration, in the event of an employee status or attribute change, or to replace a PIV card that has been compromised, lost, stolen, or damaged.

3.8.5 Special Rule for Name Change by Cardholder

See Section 2.9.1 of FIPS 201-2 for details

3.8.6 PIV Card Post Issuance Update Requirements

A PIV card post issuance update may be performed without replacing the PIV card in cases where none of the printed information on the surface of the card is changed.

3.8.7 PIV Card Verification Data Reset

The personal identification number (PIN) on a PIV card may need to be reset if the cardholder has forgotten the PIN or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency.

NOTE: If the cardholder knows their current PIN they may elect to change it using a card reader with PIN pad that supports PIN change operations. In other words, this type of operation can be done locally without an interface to the department or agency card management system.

FIPS 201-2 requires authentication of the cardholder using a 1:1 biometric match prior to performing a PIN reset. In cases where a biometric match is not possible, the cardholder shall provide the PIV card to be reset and another primary identity source document.

3.8.8 PIV Card Termination Requirements

See Section 2.9.4 of FIPS 201-2 for details

3.9 Derived PIV Credentials Issuance Requirements

Valid PIV cards may be used as the basis for issuing derived PIV credentials in accordance with NIST Special Publication 800-157, *Guidelines for Derived Personal Identity Verification (PIV) Credentials* [SP 800-157]. When a cardholder's PIV card is terminated as specified in Section 2.9.4 of FISP 201-2, any derived PIV credentials issued to the cardholder shall also be terminated.

3.10 PIV Privacy Requirements

HSPD-12 explicitly states that “protect[ing] personal privacy” is a requirement of the PIV system. As such, all departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this Standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002 [E-Gov], the Privacy Act of 1974 [PRIVACY], and OMB Memorandum M-03-22 [OMB0322], as applicable.

Departments and agencies may have a wide variety of uses of the PIV system and its components that were not intended or anticipated by the President in issuing [HSPD-12]. In considering whether a proposed use of the PIV system is appropriate, departments and agencies shall consider the aforementioned control objectives and the purpose of this Standard, namely “to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy” [HSPD-12]. No department or agency shall implement a use of the identity credential inconsistent with these control objectives.

To ensure the privacy throughout PIV lifecycle, departments and agencies shall do the following:

- Assign an individual to the role of privacy official. The privacy official is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the Standard. The individual serving in this role shall not assume any

other operational role in the PIV system.

- Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing PII for the purpose of implementing PIV, consistent with the methodology of [E-Gov] and the requirements of [OMB0322]. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.
- Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, PII), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. Provide PIV applicants full disclosure of the intended uses of the information associated with the PIV Card and the related privacy implications.
- Assure that systems that contain PII for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY].
- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.
- Ensure that only personnel with a legitimate need for access to PII in the PIV system are authorized to access the PII, including but not limited to information and databases maintained for registration and credential issuance.
- Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.
- Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.
- Utilize security controls described in [SP 800-53], *Recommended Security Controls for Federal Information Systems*, to accomplish privacy goals, where applicable.
- Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of PII. Agencies may choose to deploy PIV Cards with electromagnetically opaque holders or other technology to protect against any unauthorized contactless access to information stored on a PIV Card.

4 PIV System Overview

Note: The following section was extracted from the NIST publication, Federal Information Processing Standard Publication 201 (FIPS 201-2), "Personal Identity Verification (PIV) of Federal Employees and Contractors, Part 2," August 2013

The PIV system is composed of components and processes that support a common (smart card-based) platform for identity authentication across Federal departments and agencies for access to multiple types of physical and logical access environments. The specifications for the PIV components in this FIPS 201-2 [Standard] promote uniformity and interoperability among the various PIV system components, across departments and agencies, and across installations. The specifications for processes in this Standard are a set of minimum requirements for the various activities that need to be performed within an operational PIV system. When implemented in accordance with this Standard, the PIV card supports a suite of authentication mechanisms that can be used consistently across departments and agencies. The authenticated identity information can then be used as a basis for access control in various Federal physical and logical access environments. The following sections briefly discuss the functional components of the PIV system and the lifecycle activities of the PIV card.

4.1 Functional Components

An operational PIV system can be logically divided into the following three major subsystems:

- **PIV Front-End Subsystem**—PIV card, card and biometric readers, and PIN input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.
- **PIV Card Issuance and Management Subsystem**—the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure (PKI) directory, certificate status servers) required as part of the verification infrastructure.
- **PIV Relying Subsystem**—the physical and logical access control systems, the protected resources, and the authorization data.

The PIV relying subsystem becomes relevant when the PIV card is used to authenticate a cardholder who is seeking access to a physical or logical resource. Although this Standard does not provide technical specifications for this subsystem, various mechanisms for identification and authentication are defined in Section 6 of FIPS 201-2 to provide consistent and secure means for performing the authentication function preceding an access control decision.

Figure 1 illustrates a notional model for the operational PIV system, identifying the various system components and the direction of data flow between these components. The boundary shown in the figure is not meant to preclude FIPS 201 requirements on systems outside these boundaries.

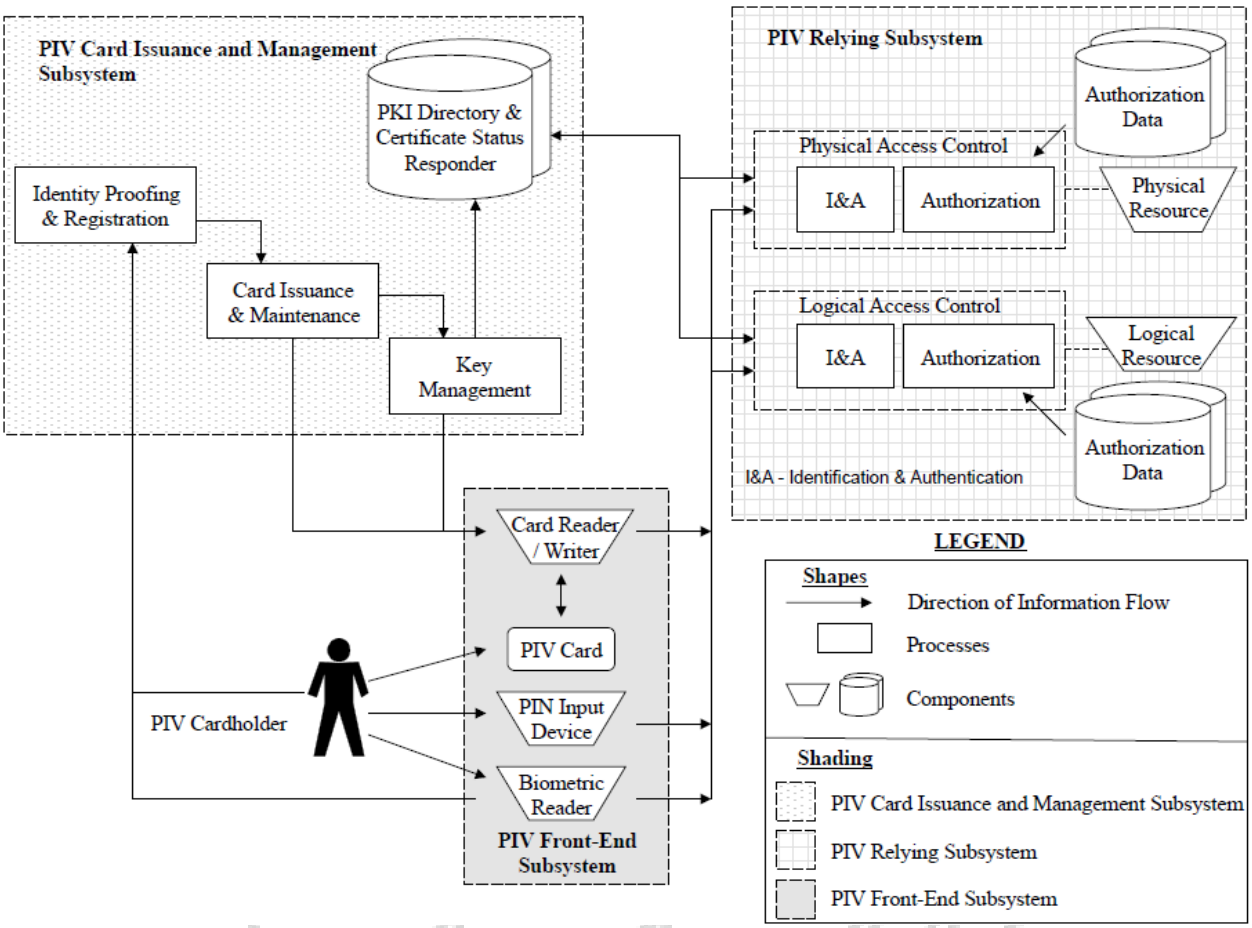


Figure 1. PIV System Notional Model from FIPS 201-2

4.1.1 PIV Front-End System

The PIV card will be issued to the applicant when all identity proofing, registration, and issuance processes have been completed. The PIV card has a credit card-size form factor, with one or more embedded integrated circuit chips (ICC) that provide memory capacity and computational capability. The PIV card is the primary component of the PIV system. The holder uses the PIV card for authentication to various physical and logical resources.

Card readers are located at access points for controlled resources where a cardholder may wish to gain access (physical and logical) by using the PIV card. The reader communicates with the PIV card to retrieve the appropriate information, located in the card's memory, to relay it to the access control systems for granting or denying access.

Card writers, which are very similar to the card readers, personalize and initialize the information stored on PIV cards. Card writers may also be used to perform remote PIV card updates. The data to be stored on PIV cards includes personal information, certificates, cryptographic keys, the PIN, and biometric data, and is discussed in further detail in subsequent sections.

PIN input devices can be used along with card readers when a higher level of authentication assurance is required. The cardholder presenting the PIV card must type in his or her PIN into the PIN input device. For physical access, the PIN is typically entered using a PIN pad device; a keyboard is generally used for logical access. The input of a PIN provides a “something you know”[17] authentication factor that activates the PIV card and enables access to other credentials resident on the card that provide additional factors of

authentication. A cryptographic key and certificate, for example, provides an additional authentication factor of “something you have” (i.e., the card) through PKI-based authentication.

Biometric readers may be located at secure locations where a cardholder may want to gain access. These readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its comparison with a real-time biometric sample. The use of biometrics provides an additional factor of authentication (“something you are”) in addition to entering the PIN (“something you know”) and providing the card (“something you have”) for cryptographic key-based authentication. This provides for a higher level of authentication assurance.

4.1.2 PIV Card Issuance and Management Subsystem

The identity proofing and registration component refers to the process of collecting, storing, and maintaining all information and documentation that are required for verifying and assuring the applicant’s identity. Various types of information are collected from the applicant at the time of registration.

The card issuance and maintenance component deals with the personalization of the physical (visual surface) and logical (contents of the ICC) aspects of the card at the time of issuance and maintenance thereafter. This includes printing photographs, names, and other information on the card and loading the relevant card applications, biometrics, and other data.

The key management component is responsible for the generation of key pairs, the issuance and distribution of digital certificates containing the public keys of the cardholder, and management and dissemination of certificate status information. The key management component is used throughout the lifecycle of PIV cards—from generation and loading of authentication keys and PKI credentials, to usage of these keys for secure operations, to eventual reissuance or termination of the card. The key management component is also responsible for the provisioning of publicly accessible repositories and services (such as PKI directories and certificate status responders) that provide information to the requesting application about the status of the PKI credentials.

4.1.3 PIV Relying Subsystem

The PIV relying subsystem includes components responsible for determining a particular PIV cardholder’s access to a physical or logical resource. A physical resource is the secured facility (e.g., building, room, parking garage) that the cardholder wishes to access. The logical resource is typically a network or a location on the network (e.g., computer workstation, folder, file, database record, software program) to which the cardholder wants to gain access.

The authorization data component comprises information that defines the privileges (authorizations) possessed by entities requesting to access a particular logical or physical resource. An example of this is an access control list (ACL) associated with a file on a computer system.

The physical and logical access control system grants or denies access to a particular resource and includes an identification and authentication (I&A) component as well as an authorization component.

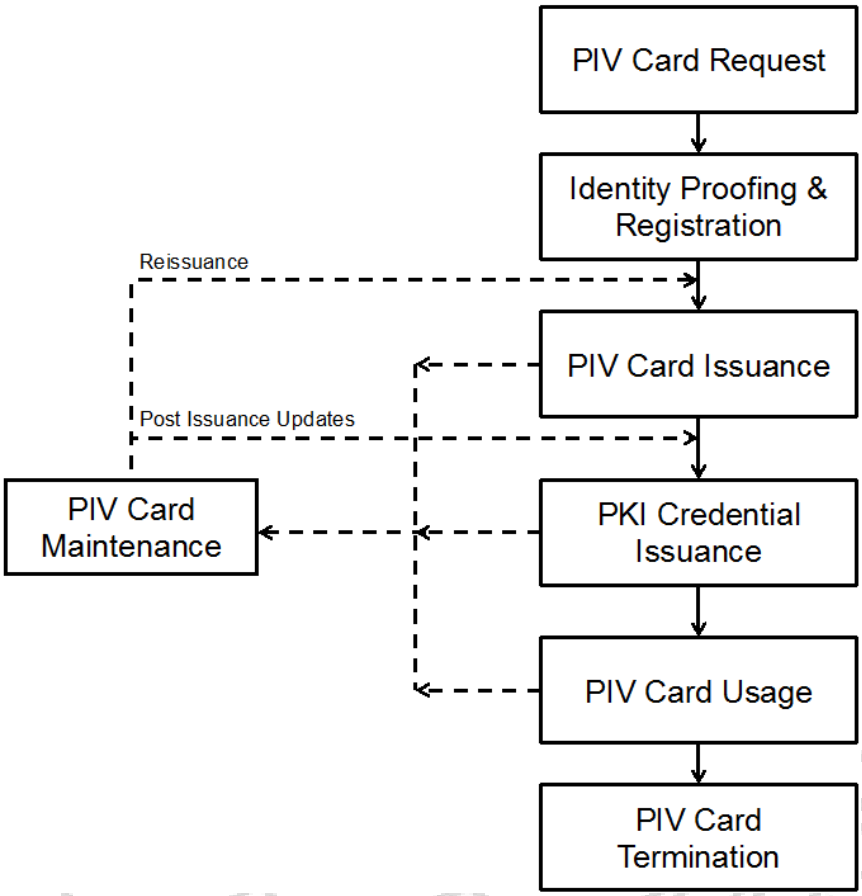
The I&A component interacts with the PIV card and uses mechanisms discussed in Section 6 of FIPS 201-2 to identify and authenticate cardholders. Once authenticated, the I&A component passes information to the authorization component which in turn interacts with the authorization data component to match the cardholder information to the information on record. Access control components typically interface with the card reader, the PIN input device, the biometric reader, supplementary databases, and any certificate status service.

4.2 PIV Card Lifecycle Activities

The PIV Card lifecycle consists of seven activities. The activities that take place during fabrication and pre-personalization of the card at the manufacturer are not considered a part of this lifecycle model.

Figure 2 (Figure 3-2 from FIPS 201-2, shown below) presents these PIV activities and depicts the PIV card request as the initial activity and PIV card termination as the end of life.

Figure 2. PIV Card Lifecycle Activities



Descriptions of the seven card lifecycle activities are as follows:

- **PIV Card Request.** This activity applies to the initiation of a request for the issuance of a PIV Card to an applicant and the validation of this request.
- **Identity Proofing and Registration.** The goal of this activity is to verify the claimed identity of the applicant, verify that the entire set of identity source documents presented at the time of registration is valid, capture biometrics, and optionally create the chain-of-trust record.
- **PIV Card Issuance.** This activity deals with the personalization (physical and logical) of the card and the issuance of the card to the intended applicant.
- **PKI Credential Issuance.** This activity deals with generating logical credentials and loading them onto the PIV Card.
- **PIV Card Usage.** During this activity, the PIV Card is used to perform cardholder authentication for access to a physical or logical resource. Access authorization decisions are made after successful cardholder identification and authentication.
- **PIV Card Maintenance.** This activity deals with the maintenance or update of the physical card and the data stored thereon. Such data includes various card applications, PINs, PKI credentials, and biometrics.
- **PIV Card Termination.** The termination process is used to permanently destroy or invalidate the PIV Card and the data and keys needed for authentication so as to prevent any future use of the card for

authentication.

5 PIV Front-End Subsystem

Note: The following section was extracted from the NIST publication, Federal Information Processing Standard Publication 201 (FIPS 201-2), Personal Identity Verification (PIV) of Federal Employees and Contractors, Part 2, Section 4, August 2013.

5.1 PIV Card Physical Characteristics

References to the PIV Card in this section pertain to the physical characteristics only. References to the front of the card apply to the side of the card that contains the electronic contacts; references to the back of the card apply to the opposite side from the front side.

The PIV Card's physical appearance and other characteristics should balance the need to have the PIV Card commonly recognized as a Federal identification card while providing the flexibility to support individual department and agency requirements. Having a common look for PIV Cards is important in meeting the objectives of improved security and interoperability. In support of these objectives, consistent placement of printed components and technology is generally necessary.

The PIV Card shall comply with physical characteristics as described in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443].

5.1.1 Printed Material

The printed material shall not rub off during the life of the PIV Card, nor shall the printing process deposit debris on the printer rollers during printing and laminating. Printed material shall not interfere with the contact and contactless ICC(s) and related components, nor shall it obstruct access to machine-readable information.

5.1.2 Tamper Proofing and Resistance

The PIV Card shall contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. At a minimum, a PIV Card shall incorporate one such security feature. Examples of these security features include the following:

- Optical varying structures;
- Optical varying inks;
- Laser etching and engraving;
- Holograms; holographic images; and
- Watermarks.

Incorporation of security features shall:

- Be in accordance with durability requirements;
- Be free of defects, such as fading and discoloration;
- Not obscure printed information; and
- Not impede access to machine-readable information.

Departments and agencies may incorporate additional tamper-resistance and anti-counterfeiting methods. As a generally accepted security procedure, Federal departments and agencies are strongly encouraged to periodically review the viability, effectiveness, and currency of employed tamper resistance and anti-counterfeiting methods.

5.1.3 Physical Characteristics and Durability

The following list describes the physical requirements for the PIV Card.

- The PIV Card shall contain a contact and a contactless ICC interface.
- The card body shall be white in accordance with color representation in Section 4.1.5 of FIPS 201-2. Only a security feature, as described in Section 4.1.2 of FIPS 201-2, may modify the perceived color slightly. Presence of a security feature shall not prevent the recognition of white as the principal card body color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.
- The card body structure shall consist of card material(s) that satisfy the card characteristics in [ISO7810] and test methods in American National Standards Institute (ANSI) 322 [ANSI322]. Although the [ANSI322] test methods do not currently specify compliance requirements, the tests shall be used to evaluate card material durability and performance. The [ANSI322] tests minimally shall include card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet light exposure, and a laundry test. Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture.
- The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect 2000 hours of southwestern United States' sunlight exposure in accordance with [ISO10373], Section 5.12. Concentrated sunlight exposure shall be performed in accordance with [G90-98] and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading resistance and subjected to the same [ISO10373] dynamic bending test.
- There are methods by which proper card orientation can be indicated. Section 4.1.4.3 of FIPS 201-2, for example, defines Zones 21F and 22F, where card orientation features may be applied. *Note: If an agency determines that tactilely discernible markers for PIV Cards impose an undue burden, the agency must implement policies and procedures to accommodate employees and contractors with disabilities in accordance with Sections 501 and 504 of the Rehabilitation Act.*
- The card shall be 27- to 33-mil thick (before lamination) in accordance with [ISO7810].
- The PIV Card shall not be embossed.
- Decals shall not be adhered to the card.
- Departments and agencies may choose to punch an opening in the card body to enable the card to be
  oriented by touch or to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted. Departments and agencies are strongly encouraged to ensure such alterations do not:
  - Compromise card body durability requirements and characteristics;
  - Invalidate card manufacturer warranties or other product claims;
  - Alter or interfere with printed information, including the photo; or
  - Damage or interfere with machine-readable technology, such as the embedded antenna.
- The card material shall withstand the effects of temperatures required by the application of a polyester
  laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer shall not interfere with the smart card reader operation. The

card material shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.

- The PIV Card may be subjected to additional testing.

5.2 Visual Card Topography[13]

The information on a PIV Card shall be in visual printed and electronic form. This section covers the placement of visual and printed information. It does not cover information stored in electronic form, such as stored data elements, and other possible machine-readable technologies. Logically stored data elements are discussed in Section 4.2 of FIPS 201-2.

As noted in Section 4.1.3 of FIPS 201-2, the PIV Card shall contain a contact and a contactless ICC interface. This Standard does not specify whether a single chip is used or multiple chips are used to support the mandated contact and contactless interfaces.

To achieve a common PIV Card appearance, yet provide departments and agencies the flexibility to augment the card with department or agency-specific requirements, the card shall contain mandated and optional printed information and mandated and optional machine-readable technologies. Mandated and optional items shall generally be placed as described and depicted. Printed data shall not interfere with machine-readable technology.

Areas that are marked as reserved should not be used for printing. The reason for the recommended reserved areas is that placement of the embedded contactless ICC module may vary from manufacturer to manufacturer, and there are constraints that prohibit printing over the embedded contactless module. The PIV Card topography provides flexibility for placement of the embedded module, either in the upper right-hand corner or in the lower bottom portion. Printing restrictions apply only to the area where the embedded module is located (i.e., upper right-hand corner, lower bottom portion).

Because technological developments may obviate the need to have a restricted area, or change the size of the restricted area, departments and agencies are encouraged to work closely with card vendors and manufacturers to ensure current printing procedures and methods are applied as well as potential integration of features that may improve tamper resistance and anti-counterfeiting of the PIV Card.

Figure 3 and below on the next page show some of the possible topographies allowed for the PIV Card front and back. For a complete description of all allowed configurations, refer to FIPS 201-2 sections 4.1.4 to 4.1.5, pages 25 to 39.

[13] Content in this section was extracted from Federal Information Processing Standard Publication 201 (FIPS 201-2), "Personal Identity Verification (PIV) of Federal Employees and Contractors," Section 4.1, August 2013

Figure 3. PIV Card Front

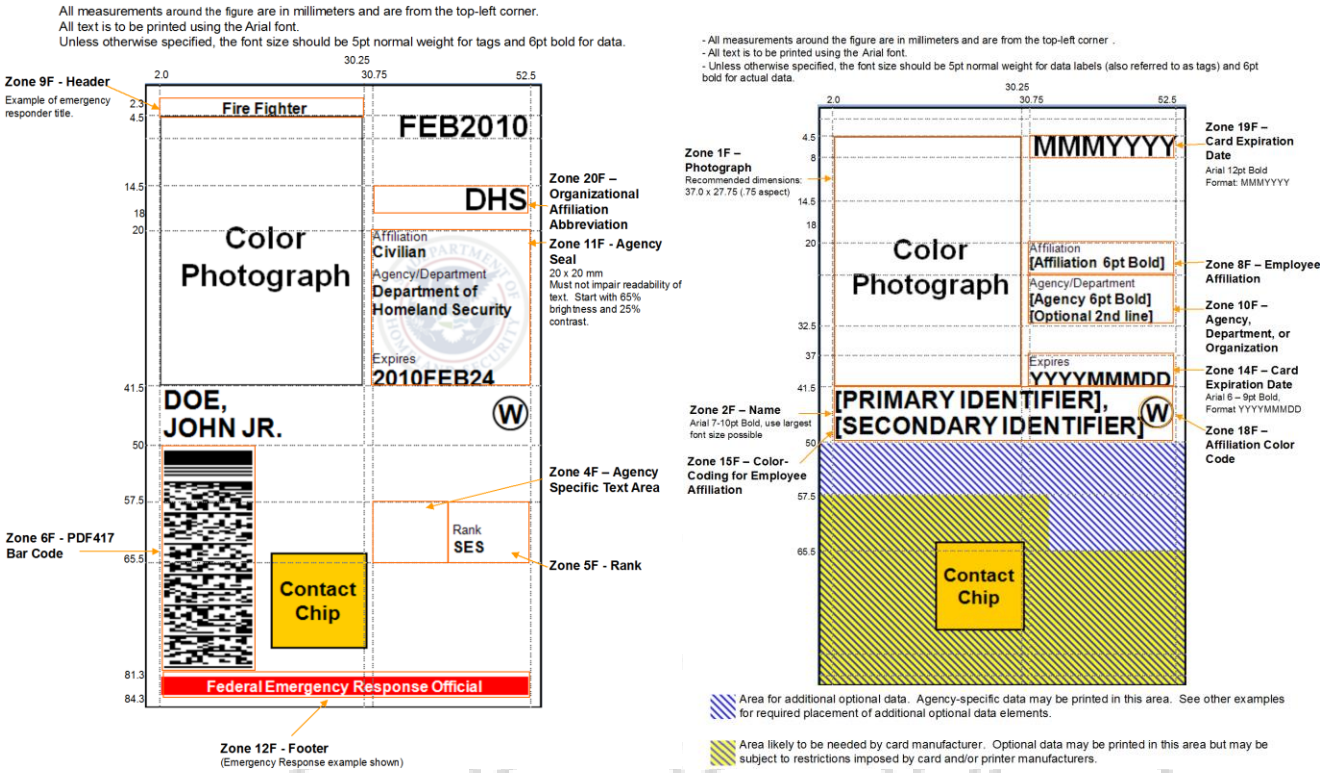


Figure 4. PIV Card Back

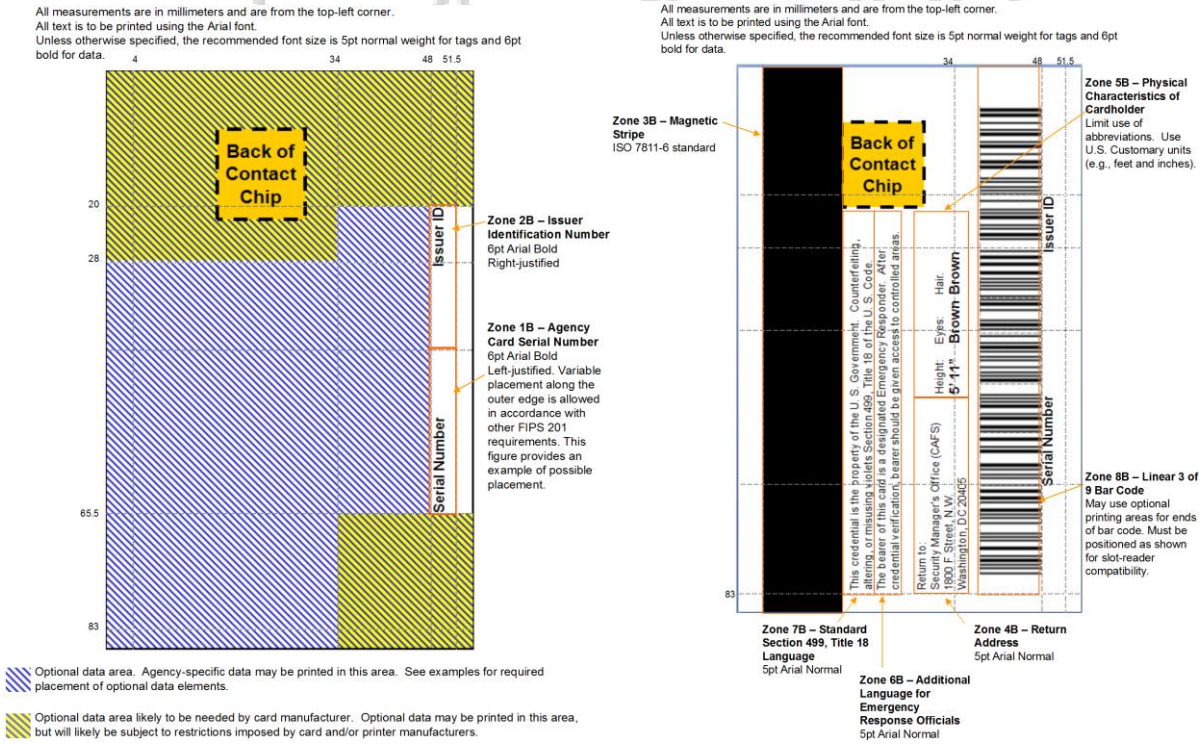


***Table 1*. PIV Card Mandatory and Optional Printed Zones and Features**

	Mandatory Items	Optional Items
PIV Card Front	1F - Photograph: full frontal pose from top of head to shoulder (300 dots per inch minimum) 2F - Full name 8F - Employee affiliation 10F - Organizational affiliation 14F - Card Expiration date (YYYYMMMDD) 15F - Color Coding for Employee Affiliation (background for name zone) 18F - Affiliation Color Code 19F - Card Expiration date (MMMYYYY)	3F - Signature 4F - Agency-specific text 5F - Rank 6F - PDF two-dimensional bar code 9F - Header 11F - Agency seal 12F - Footer 13F - Issue date (YYYYMMMDD) 16F - Photo border for employee affiliation 17F - Agency specific data 20F - Organization Affiliation Abbreviation 21F - Edge Ridging or Notched Tactile Marker 22F - Laser Engraved Tactile Marker
PIV Card Back	1B - Agency card serial number 2B - Issuer identification (6 characters for department code, 4 characters for agency code, 5 digit number identifying issuing facility)	3B - Magnetic stripe 4B - Return Address 5B - Physical characteristics of cardholder 6B - Additional language for emergency responder officials 7B - Standard Section 499, Title 18 language, warning against counterfeiting, altering or misusing the card 8B - Linear 3 of 9 bar code 9B & 10 B - Agency-specific text

5.3 PIV Card Logical Characteristic

This section defines logical identity credentials and the requirements for use of these credentials.

To support a variety of authentication mechanisms, the PIV Card shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. The following mandatory data elements are part of the data model for PIV logical credentials that support authentication mechanisms interoperable across agencies.

Mandatory elements used in authentication mechanisms are:

- A PIN;
- A CHUID;
- PIV authentication data (one asymmetric private key and corresponding certificate);
- Two fingerprint templates;
- An electronic facial image; and
- Card authentication data (one asymmetric private key and corresponding certificate).

This Standard also defines two data elements for the PIV data model that are mandatory if the cardholder has a government-issued email account at the time of credential issuance.

Conditional elements used in authentication mechanisms are:

- An asymmetric private key and corresponding certificate for digital signatures; and
- An asymmetric private key and corresponding certificate for key management.

This Standard also defines optional data elements for the PIV data model.

Optional elements used in authentication mechanisms are:

- One or two iris images;
- One or two fingerprint templates for on-card comparison;
- A symmetric Card Authentication key for supporting physical access applications; and
- A symmetric PIV Card Application Administration key associated with the card management system.
- An asymmetric PIV secure messaging key associated with its signer certificate data object.

In addition to the above, other data elements are specified in [SP 800-73].

PIV logical credentials fall into the following three categories:

1. Credential elements used to prove the identity of the cardholder to the card (CTC authentication);
2. Credential elements used to prove the identity of the card management system to the card (CMTC authentication); and
3. Credential elements used by the card to prove the identity of the cardholder to an external entity (CTE authentication) such as a host computer system.

The PIN falls into the first category, the PIV Card Application Administration Key into the second category, and the CHUID, biometric credentials, symmetric keys, and asymmetric keys into the third. The fingerprint templates for on-card comparison fall into the first and third categories.

5.4 PIV Card Activation

The PIV Card must be activated[14] to perform privileged[15] operations such as reading biometric information and using asymmetric keys. The PIV Card must be activated for privileged operations only after authenticating the cardholder or the appropriate card management system.

5.4.1 Activation by Cardholder

PIV Cards shall implement user-based cardholder activation to allow privileged operations using PIV credentials held by the card. At a minimum, the PIV Card shall implement PIN-based cardholder activation in support of interoperability across departments and agencies. Other card activation mechanisms (e.g., OCC card activation), only as specified in [SP 800-73], may be implemented and shall be discoverable. For PIN-based cardholder activation, the cardholder shall supply a numeric PIN. The verification data shall be transmitted to the PIV Card and checked by the card. If the verification data check is successful, the PIV Card is activated. The PIV Card shall include mechanisms to block activation of the card after a number of consecutive failed activation attempts. The number of allowable consecutive failed activation attempts may vary by activation mechanism.

The PIN should not be easily guessable or otherwise individually identifiable in nature (e.g., part of a Social Security number, phone number). The required PIN length shall be a minimum of six digits.

[14] Activation in this context refers to the unlocking the PIV Card so privileged operations can be performed.
[15] A read of a PIV CHUID is not considered a privileged operation.

5.4.2 Activation by Card Management System

PIV Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP 800-73]. When cards are personalized, PIV Card Application Administration Keys shall be set to be specific to each PIV Card. That is, each PIV Card shall contain a unique PIV Card Application Administration Key. PIV Card Application Administration Keys shall meet the algorithm and key size requirements stated in SP 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification.[16]

5.5 PIV Data Model Elements[17]

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

A PIV Card application contains seven mandatory interoperable data objects, two conditional interoperable data objects and may contain twenty four optional interoperable data objects.

The seven mandatory data objects for interoperable use are as follows:

1. Card Capability Container
2. Card Holder Unique Identifier (CHUID)
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 conditional data objects for interoperable use are as follows:

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

The 27 optional data objects for interoperable use are as follows:

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

[16] NIST Special Publication 800-78-3, "Cryptographic Algorithms and Key Sizes for Personal Identity Verification" (SP 800-78), December 2010 http://csrc.nist.gov/publications/PubsSPs.html

[17] Content in this section was extracted from: NIST SP 800-73-4 (Draft); FIPS 201-2 and "Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems," Smart Card Alliance white paper, September 2005

5.5.1 Mandatory Data Elements

The seven mandatory data objects support FIPS 201-2 minimum mandatory compliance. The following briefly describes each data object.

5.5.1.1 Card Capability Container

The Card Capability Container (CCC) is a mandatory data object whose purpose is to facilitate compatibility of Government Smart Card Interoperability Specification (GSC-IS)[18] applications with end-point PIV Cards.

The CCC supports minimum capability for retrieval of the data model and optionally the application information as specified in 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 the SP 800-73-4 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 data elements of the CCC, except for the data model number, may optionally have a length value set to zero bytes (i.e., no value field will be supplied). The content of the CCC data elements, other than the data model number, are out of scope for this specification.

5.5.1.2 Card Holder Unique Identifier (CHUID)

One of the important identifiers used by FIPS 201 applications is a standardized data model for cardholder identification data. This data model, represented by the CHUID, was first defined by Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems (TIG SCEPACS)[19] and subsequently expanded in NIST SP 800-73. The CHUID includes two required unique identifiers: the Federal Agency Smart Credential Number (FASC-N) and the Global Unique Identification Number (GUID), which both uniquely identifies each card. Note: As required by FISP 201-2, both unique identifier (FASC-N and GUID UUID) shall be used as binding elements in all certificates of a given card

The CHUID must be written to the FIPS 201-compliant card chip or chips and be available from both the contact and contactless interfaces. All of the CHUID elements, when present, must contain values. The reason for including all of this information in the CHUID is to identify each card uniquely within the Federal government.

Table 2 describes the data elements within the CHUID[20].

[18] NIST Interagency Report 6887, "Government Smart Card Interoperability Specification," Version 2.1, July 2003, http://csrc.nist.gov/publications/nistir/nistir-6887.pdf

[19] "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems" (TIG SCEPACS), Physical Access Interagency Interoperability Working Group, Government Smart Card Interagency Advisory Board, July 30, 2004, http://fips201ep.cio.gov/documents/TIG_SCEPACS_v2.2.pdf

[20] The CHUID is defined as Tag '5FC102' in the container 0x3000, always read and accessible on both contact and contactless interfaces.

Table 2: CHUID Data Model Definition[21]

Data Element (TLV)	Tag	Type	Max. Bytes [22]
Buffer Length (Optional) *	0xEE	Fixed	2
Federal Agency Smart Credential Number (FASC-N)	0x30	Fixed Text	25
Organization Identifier (Optional) *	0x32	Fixed	4
DUNS (optional) *	0x33	Fixed	9
Global Unique Identifier (GUID)	0x34	Fixed Numeric	16
Expiration Date	0x35	Date (YYYYMMDD)	8
Issuer Asymmetric Signature	0x3E	Variable	2816
Error Detection Code	0xFE	LRC	0

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

The Asymmetric Signature Field in the CHUID is a very important element of the trust, allowing the path to be built from the issuer to any verifier of the PIV Card.

5.5.1.3 X.509 Certificate for PIV Authentication

The X.509 Certificate for PIV Authentication and its associated private key, as defined in FIPS 201-2, is used to authenticate the card and the cardholder. The PIV Authentication private key and its corresponding certificate are only available over the contact interface or Virtual Contact Interface (VCI). The read access control rule for the X.509 Certificate for PIV Authentication is “Always,” meaning the certificate can be read without access control restrictions. The Public Key Infrastructure (PKI) cryptographic function (see Table 3) is protected with a 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.

5.5.1.4 X.509 Certificate for Card Authentication

FIPS 201 specifies the mandatory asymmetric Card Authentication key (CAK) as a private key that may be used to support physical access applications. The read access control rule of the corresponding X.509 Certificate for Card Authentication is “Always,” meaning the certificate can be read without access control restrictions. The PKI cryptographic function is under an “Always” access rule, and thus private key operations can performed without access control restrictions. The asymmetric CAK is generated by the PIV Card issuer in accordance with FIPS 140-2 requirements for key generation. An asymmetric CAK

[21] NIST Special Publication 800-73-4 (Draft): "Interfaces for Personal Identity Verification," Table 9.

[22] The number of bytes listed for each data element is provided as maximum number of bytes. For example, a 4-digit agency code will never take up more than 4 bytes, but it may be stored in 2 bytes if encoded as 4 bits per digit. The data in the FASC-N requires over 32 digits, but is stored in just 25 bytes due to the encoding technique employed.

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.

5.5.1.5 Cardholder Fingerprints

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

5.5.1.6 Cardholder Facial Image

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

5.5.1.7 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 Container IDs 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.

5.5.2 Conditional Data Elements

5.5.2.1 X.509 Certificate for Digital Signature

The X.509 Certificate for Digital Signature and its associated private key, as defined in FIPS 201, support the use of digital signatures for the purpose of document signing. The digital signature private key and its corresponding certificate are only available over the contact interface or VCI. The read access control rule for the X.509 Certificate for digital signing is “Always,” meaning the certificate can be read without access control restrictions. The PKI cryptographic function (see Table 3) is protected with a “PIN Always” or “OCC Always” access rule. In other words, the PIN or OCC data must be submitted and verified every time immediately before a digital signature key operation. This ensures cardholder participation every time the private key is used for digital signature generation.

5.5.2.2 X.509 Certificate for Key Management

The X.509 Certificate for Key Management and its associated private key, as defined in FIPS 201, support the use of encryption for the purpose of confidentiality. The key management private key and its corresponding certificate are only available over the contact interface or VCI. This key pair may be escrowed by the issuer for key recovery purposes. The read access control rule for the X.509 certificate is “Always,” meaning the certificate can be read without access control restrictions. The PKI cryptographic function (see Table 3) is protected with a “PIN” or “OCC” access rule. In other words, once the PIN or OCC data is submitted and verified, subsequent key management key operations can be performed without requiring the PIN or OCC data again. This enables multiple private key operations without additional cardholder consent.

5.5.3 Optional Data Elements

NIST SP 800-73-4 specifies twenty-seven optional data elements.

5.5.3.1 Printed Information

All FIPS 201 mandatory information printed on the card is duplicated on the chip in this data object. The printed information data object shall not be modified post-issuance[23]. The Security Object enforces

[23] As the content of the printed information data object represents what is printed on the card, it cannot vary over time.

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.

5.5.3.2 Discovery Object

The Discovery Object, if implemented, is the 0x7E interindustry ISO/IEC 7816-6 template that nests interindustry data objects. For the Discovery Object, the 0x7E template nests two mandatory BER-TLV structured interindustry data elements:

1) tag 0x4F contains the AID of the PIV Card Application and
2) tag 0x5F2F lists the PIN Usage Policy.

Note: One bit in the discovery object is reserved to indicate when the pairing code is not used in the establishment of the VCI. Agencies not using the Paring code for the VCI must have a special authorization.

5.5.3.3 Key History Object

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

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

5.5.3.4 Retired X.509 Certificates for Key Management

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

5.5.3.5 Cardholder Iris Images

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

5.5.3.6 Biometric Information Templates Group Template

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

5.5.3.7 Secure Messaging Certificate Signer

The Secure Messaging Certificate Signer data object, which shall be present if the PIV Card supports secure messaging for non-card-management operations, contains the certificate(s) needed to verify the signature on the secure messaging card verifiable certificate (CVC), as specified in SP 800-73-4 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 73-4 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.

5.5.3.8 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 in SP 800-74 Part 1).

5.5.4 Inclusion of Universally Unique IDentifiers (UUIDs)

SP 800-73-4 provides support for two UUIDs on a PIV Card. Both should be 16-byte binary representation of a valid UUID version 1, 4, or 5, as specified in [RFC4122, Section 4.1.3][24].

The Card UUID is the value of the GUID data object in the CHUID. It is an identifier unique to each card, and shall be present on all PIV Cards.

The CardHolder UUID is a persistent identifier for the cardholder, and it is optional to implement in PIV Cards. The use of such identifier is to allow traceability of a given cardholder between multiple PIV Cards he owns over time, allowing for example, a PACS to transfer an existing authorization to the new PIV Card of the same cardholder. There a privacy risk using such a permanent identifier though, as it allows third parties to track actions of a given individual over time, even when his/her PIV Card is changed.

5.5.5 Data Object Containers and associated Access Rules and Interface Modes

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

***Table 3*. Data Model Containers**

Container Name	Container ID	Access Rule for Read	Contact/ Contactless	BER-TLV Tag	M/O/C
Card Capability Container	0xDB00	Always	Contact	5FC107	M
Card Holder Unique Identifier	0x3000	Always	Contact & Contactless	5FC102	M
X.509 Certificate for PIV Authentication	0x0101	Always	Contact	5FC105	M
X.509 Certificate for Card Authentication	0x0500	Always	Contact & Contactless	5FC101	M
Cardholder Fingerprints	0x6010	PIN	Contact	5FC103	M
Security Object	0x9000	Always	Contact	5FC106	M
Cardholder Facial Image	0x6030	PIN	Contact	5FC108	M
X.509 Certificate for Digital Signature	0x0100	Always	Contact	5FC10A	C

[24] A null value of the UUID of the GUID (card UUID) is not permitted by SP 800-73-4.

Container Name	Container ID	Access Rule for Read	Contact/ Contactless	BER-TLV Tag	M/O/C
X.509 Certificate for Key Management	0x0102	Always	Contact	5FC10B	C
Printed Information	0x3001	PIN or OCC	Contact	5FC109	O
Discovery Object	0x6050	Always	Contact & Contactless	7E	O
Key History Object	0x6060	Always	Contact	5FC10C	O
Retired X.509 Certificate for Key Management 1	0x1001	Always	Contact	5FC10D	O
Retired X.509 Certificate for Key Management 2	0x1002	Always	Contact	5FC10E	O
Retired X.509 Certificate for Key Management 3	0x1003	Always	Contact	5FC10F	O
Retired X.509 Certificate for Key Management 4	0x1004	Always	Contact	5FC110	O
Retired X.509 Certificate for Key Management 5	0x1005	Always	Contact	5FC111	O
Retired X.509 Certificate for Key Management 6	0x1006	Always	Contact	5FC112	O
Retired X.509 Certificate for Key Management 7	0x1007	Always	Contact	5FC113	O
Retired X.509 Certificate for Key Management 8	0x1008	Always	Contact	5FC114	O
Retired X.509 Certificate for Key Management 9	0x1009	Always	Contact	5FC115	O
Retired X.509 Certificate for Key Management 10	0x100A	Always	Contact	5FC116	O
Retired X.509 Certificate for Key Management 11	0x100B	Always	Contact	5FC117	O
Retired X.509 Certificate for Key Management 12	0x100C	Always	Contact	5FC118	O
Retired X.509 Certificate for Key Management 13	0x100D	Always	Contact	5FC119	O
Retired X.509 Certificate for Key Management 14	0x100E	Always	Contact	5FC11A	O
Retired X.509 Certificate for Key Management 15	0x100F	Always	Contact	5FC11B	O
Retired X.509 Certificate for Key Management 16	0x1010	Always	Contact	5FC11C	O
Retired X.509 Certificate for Key Management 17	0x1011	Always	Contact	5FC11D	O
Retired X.509 Certificate for Key Management 18	0x1012	Always	Contact	5FC11E	O
Retired X.509 Certificate for Key Management 19	0x1013	Always	Contact	5FC11F	O
Retired X.509 Certificate for Key Management 20	0x1014	Always	Contact	5FC120	O
Cardholder Iris Image	0x1015	PIN	Contact	5FC121	O
Biometric Information Template Group Template	0x1016	Always	Contact & Contactless	7F61	O
Secure Messaging Certificate Signer	0x1017	Always	Contact & Contactless	5FC122	O
Pairing Code reference data Container	0x1018	PIN or OCC	Contact	5FC123	O

A detailed spreadsheet of the data model with container IDs, Data objects OIDs and their tags can be found in Appendix A of SP 800-73-4

5.6 Cryptographic Specifications[25]

At a minimum, the PIV Card must store two asymmetric private keys and the corresponding public key certificates, namely the PIV Authentication key and the asymmetric Card Authentication key. The PIV Card must also store a digital signature key and a key management key, and the corresponding public key certificates, unless the cardholder does not have a government-issued email account at the time of credential issuance.

In addition, the PIV Card may include an asymmetric private key and corresponding public key certificate to establish symmetric keys for use with secure messaging, as specified in [SP 800-73] and [SP 800-78]. Secure messaging enables data and commands transmitted between the card and an external entity to

[25] Source: FIPS 201-2, pages 41-44

be both integrity protected and encrypted. Secure messaging may be used, for example, to enable the use of on-card biometric comparison as an authentication mechanism.

The PIV Card implements the following cryptographic operations and support functions:

- RSA or elliptic curve key pair generation
- RSA or elliptic curve private key cryptographic operations
- Importation and storage of X.509 certificates.

Symmetric cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a symmetric Card Authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize Advanced Encryption Standard (AES) based challenge/response for physical access, the PIV Card must contain storage for the AES key and support AES operations through the contactless interface. Algorithms and key sizes for each PIV key type are specified in [SP 800-78].

FIPS 201-2 specifies that nearly all cryptographic operations using the PIV keys are to be performed on-card[26]; the PIV Card need not implement any additional cryptographic functionality (e.g., hashing, signature verification) by additional cryptographic mechanisms implemented on-card. Algorithms and key sizes for each PIV key type are specified in SP800-78.

The PIV Card has two mandatory keys, two conditional keys and two optional keys.

- The ***PIV Authentication Key*** is an asymmetric private key supporting card authentication for an interoperable environment, and it is mandatory for each PIV Card. This key is generated on the PIV Card. The PIV Card does permit exportation of the PIV authentication key. The PIV authentication key must be available only through the contact interface and the virtual contact interface of the PIV Card. The x.509 certificate shall include in the FASC-N as well as the Card UUID (GUID Value) in the alternative name extension. In addition, the X.509 certificate shall have an extension including the status of the PIV NACI indicator at the time of card issuance. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).
- The ***Asymmetric Card Authentication key*** is mandatory in all PIV Cards; it may be generated on the PIV Card or imported securely to the card. The PIV Card shall not permit exportation of the Card Authentication key. Cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. Private key operations may be performed using this key without card activation (e.g., the PIN need not be supplied for operations with this key). As for the PIV Card Authentication Key, the x.509 certificate shall include in the FASC-N as well as the Card UUID (GUID Value) in the alternative name extension.
- The ***Symmetric Card Authentication Key*** is optional and may be imported onto the card by the issuer or be generated on the card. If present, the symmetric Card Authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]. If present**,** cryptographic operations using this key may be performed without card activation (e.g., the PIN need not be supplied for operations with this key). The cryptographic operations that use the Card Authentication Key shall be available through the contact and the contactless interfaces of the PIV Card. This Standard does not specify key management protocols or infrastructure requirements.

[26] All Asymmetric keys (except the Card Authentication Key and the Key Management Key) are required to be generated on the PIV card. For an off-card generation of the Card Authentication Key, the use of an approved FIPS 140-2 Level 3 device is mandatory.

- The ***PIV Digital Signature Key*** shall be generated on the PIV Card. The PIV Card shall not permit exportation of the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact and the virtual contact interfaces of the PIV Card. Private key operations may not be performed without explicit user action, as this Standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key
- The ***Key Management Key*** is an asymmetric private key supporting key establishment and transport, and it is optional. This can also be used as an encryption key. This key may be generated on the PIV Card or imported to the card. If present, the cryptographic operations that use the key management key must only be accessible using the contact and the virtual contact interfaces of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation). This key is sometimes called an encryption key or an encipherment key.
- The PIV Card ***Application Administrative Key*** is a key used for personalization and post-issuance activities, and it is optional. The card management key is imported onto the card by the issuer. If present, the card management key must only be accessible using the contact interface[27] of the PIV Card.

The PIV Card may also import and store X.509 certificates for use in PKI path validation. These trust anchor certificates may be accessed through the contact interface using an activated PIV Card without explicit cardholder action. If supported, initialization and update of trust anchor certificates require explicit cardholder action, in addition to activation of the card.

5.6.1 Secure Messaging and Virtual Card Interface

5.6.1.1 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 3) 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 Part 2, Section 4.1.5 of SP 800-73-4 (Draft Version). 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 of SP 800-73-4 (Draft Version).

5.6.1.2 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 5.6.1.2) on the card and may be printed on the back of the card in an agency-specific text area (Zones 9B or 10B). PIV Card issuers may choose to provide the pairing code value to the cardholder in another manner, such as printing it on a slip of paper, rather than printing it on the back of the card.

Unlike the PIV Card Application PIN or the Global PIN, there are no restrictions on the caching of the pairing code by client applications. It is recommended that a client application that needs to communicate with a PIV Card over its virtual contact interface obtain the card’s pairing code during a registration step,

[27] The use of this key over the virtual contact interface is not allowed by FIPS 201-2.

either by asking the cardholder to enter the value or by reading it from the card over the contact interface from the Pairing Code Reference Data Container, and then cache the pairing code until the card expires. The client application may then connect to the card and establish a virtual contact interface with it whenever the card is within read-range of the client application's contactless card reader without needing to prompt the cardholder.

5.6.1.3 PIV Algorithm Identifier

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

5.6.1.4 Cryptographic Mechanism Identifiers

Cryptographic Mechanism Identifiers are defined in Table 4. These identifiers serve as inputs to the GENERATE ASYMMETRIC KEY PAIR card command and the Part 3 pivGenerateKeyPair() client API function call, which initiates the generation and storage of the asymmetric key pair.

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

Table 4. Cryptographic Mechanism Identifiers

5.6.1.5 Secure Messaging

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

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

Note: The client application can verify the certificate associated with the card secure messaging asymmetric key pair used in key establishment. This provides a higher level of trust to a secure messaging session. The shared symmetrical key is used to provide (an alternate form of) card authentication in addition to the usual confidentiality and integrity security services

5.6.1.6 Virtual Contact Interface

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

5.7 Biometric Data[28]

The following biometric data shall be stored on the PIV Card:

- Two fingerprint templates. If no fingerprint images meeting the quality criteria of [SP 800-76] are available, the PIV Card shall nevertheless be populated with fingerprint records as specified in [SP 800-76].
- An electronic facial image.

The following biometric data may also be stored on the PIV Card:

- One or two iris images.
- Fingerprint templates for on-card comparison.

All biometric data shall be stored in the data elements referenced by [SP 800-73] and in conformance with the preparation and formatting specifications of [SP 800-76].

NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification* states that, at a minimum, two fingerprint templates are to be stored on the PIV Card (referred to as the PIV Card templates) and that these templates must be a conformant instance of the INCITS 378-2009 (MINUSTD) minutiae template standard[29]. These are prepared from images of the primary and secondary fingers (as specified in FIPS 201).

The templates constitute the enrollment biometrics for PIV authentication and as such are supported by a high quality image acquisition specification, and a FBI-certified compression format. The specification of a standardized template in this section enables use of the PIV Card in a multi-vendor product environment.

When a PIV Card is issued, new live fingerprints of both the primary and secondary fingers must be captured and matched with the PIV Card templates. This binds the cardholder to the individual whose background was checked.

5.7.1 Biometric Data Access

The PIV biometric data, except for fingerprint templates for on-card comparison, that is stored on the card

- Shall be readable through the contact interface and after the presentation of a valid PIN; and
- May optionally be readable through the virtual contact interface and after the presentation of a valid PIN.

On-card biometric comparison may be performed over the contact and the virtual contact interfaces of the PIV Card to support card activation (FIPS 201-2 Section 4.3.1) and cardholder authentication (FIPS 201-2 Section 6.2.2). The fingerprint templates for on-card comparison shall not be exportable.

5.7.2 On-Card Biometric Comparison (OCC)

The PIV Card Application may host the optional on-card biometric comparison algorithm. In this case, on-card biometric comparison data is stored on the card, which cannot be read, but could be used for identity verification. A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card responds with an indication of the success of the on-card biometric comparison. The response includes information that allows the reader to authenticate the card. The cardholder PIN is not required for this operation. The PIV Card shall include a mechanism to block this

[28] Sources for this section: FIPS 201; NIST Special Publication 800-76-2, "Biometric Data Specification for Personal Identity Verification," (SP 800-76-2), July 2013, http://csrc.nist.gov/publications/PubsSPs.html ; "Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems," Smart Card Alliance white paper, September 2005

[29] ANSI INCITS 378-2009, "Information technology - Finger Minutiae Format for Data Interchange"

authentication mechanism after a number of consecutive failed authentication attempts as stipulated by the department or agency. As with authentication using the PIV biometrics, if agencies choose to implement on-card biometric comparison, it shall be implemented as defined in [SP 800-73] and [SP 800-76].

Some of the characteristics of the on-card biometric comparison authentication mechanism are as follows:

- Highly resistant to credential forgery.
- Strong resistance to use of unaltered card by non-owner.
- Applicable with contact and contactless card readers.

NOTE: The OCC fingerprints should NOT be the same as used for off card biometric matches. Use of the same fingerprints for both is in effect revealing the biometric "PIN" to the outside world which defeats the security.

5.8 Card Reader Specifications[30]

This section provides minimum requirements for the contact and contactless card readers. Also, this section provides requirements for PIN input devices. Further requirements are specified in [SP 800-96].

5.8.1 Contact Reader Specifications

Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface. These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface in general desktop computing environment. Specifically, the contact card readers shall conform to the requirements specified in [SP 800-96]. In systems where the readers are not connected to general-purpose desktop computing systems, the reader-to-host system interface is not specified in this Standard.

5.8.2 Contactless Reader Specifications

Contactless card readers shall conform to [ISO14443] standard for the card-to-reader interface and data transmitted over the [ISO14443] link shall conform to [ISO7816]. In cases where these readers are connected to general-purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-host system interface. Specifically, the contactless card readers shall conform to the requirements specified in [SP 800-96]. In systems where the readers are not connected to general-purpose desktop computing systems, the reader-to-host system interface is not specified in this Standard.

5.8.3 Reader Resilience and Flexibility

The international standard ISO/IEC 24727 [ISO24727] enables a high degree of interoperability between electronic credentials and relying subsystems by means of an adaptation layer. To make interoperability among PIV system middleware, card readers, and credentials more resilient and flexible, the Department of Commerce will evaluate ISO/IEC 24727 and propose an optional profile of ISO/IEC 24727 in [SP 800-73]. The profile will explain how profile-conformant middleware, card readers, and PIV Cards can be used interchangeably with middleware, card readers, and PIV Cards currently deployed.

Specifications of the profile will become effective, as an optional means to implement PIV system readers and middleware, when OMB determines that the profile specifications are complete and ready for deployment.

5.8.4 Card Activation Device Requirements

When the PIV Card is used with OCC data or a PIN for physical access, the input device shall be

[30] Source: FIPS 201-2, pages 46-47, Section 4.4

integrated with the PIV Card reader. When the PIV Card is used with OCC data or a PIN for logical access (e.g., to authenticate to a Web site or other server), the input device is not required to be integrated with the PIV Card reader. If the input device is not integrated with the PIV Card reader, the OCC data or the PIN shall be transmitted securely and directly to the PIV Card for card activation. The specifications for fingerprint capture devices for on-card comparison are given in [SP 800-76]. Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document

6 PIV Card Issuance and Lifecycle

This section[31] describes the overall PIV system and the process for acquiring and using a PIV Card and managing the PIV Card and identity credential over its lifecycle.

FIPS 201 specifies a common platform of secure and standard practices that enables trust among the different issuers of PIV Cards. The process is composed of several key functions[32], as illustrated in Figure *5*.

- **Sponsorship**. A sponsor's duty is to vouch that an applicant has a need for a PIV Card and authorize applicant enrollment. The sponsor may also authorize the cost incurred for the credentialing process.
- **Enrollment**. The enrollment process is designed to verify the identity of an applicant in person and collect information from the applicant. Applicants must bring two forms of identification and are fingerprinted and photographed at enrollment. The information collected is used to perform suitability checks and to create the credential.
- **Adjudication**. Trusted adjudicators determine whether an applicant can receive a credential based on the results of the suitability check. Identity vetting procedures (e.g., National Agency Check–with Inquiries (NAC-I), education, employment, credit history, and verification of claimed skills) are part of the adjudication process, with disqualifiers defined as part of the vetting procedures. Passing adjudication successfully triggers credential production.
- **Credential production**. Credentials can be personalized in a centralized facility or at local issuance stations. Relevant information is printed according to Federal standards, security features are added, and the electronic smart card chip is encoded with personal data.
- **Issuance and activation**. When an applicant arrives to pick up the personalized credential, the issuer verifies the applicant's identity by re-verifying the identity documents presented at enrollment and matching the applicant's fingerprint to the one used to enroll. The credential is then "unlocked," digital certificates and a PIN are loaded into the chip, and the credential is released to the applicant for use.
- **Credential use**. Activated credentials can be used to access secure physical locations and computer networks and to validate identity and attributes electronically.

All of these process steps must be supported by both technology and policies and procedures. Only the consistent execution and enforcement of policies and procedures can ensure the overall integrity of the system.

In addition, managing credentials over their life cycle has equal importance to issuance and specific credential use cases. Both attributes and certificate revocation status must be managed over the credential lifecycle.

[31] Details may be found in document: FICAM_Roadmap_and_Implementation_Guidance_v2 0_20111202_0.pdf

[32] "Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery," Smart Card Alliance white paper, October 2008, http://www.smartcardalliance.org/pages/publications-emergency-response-official-credentials

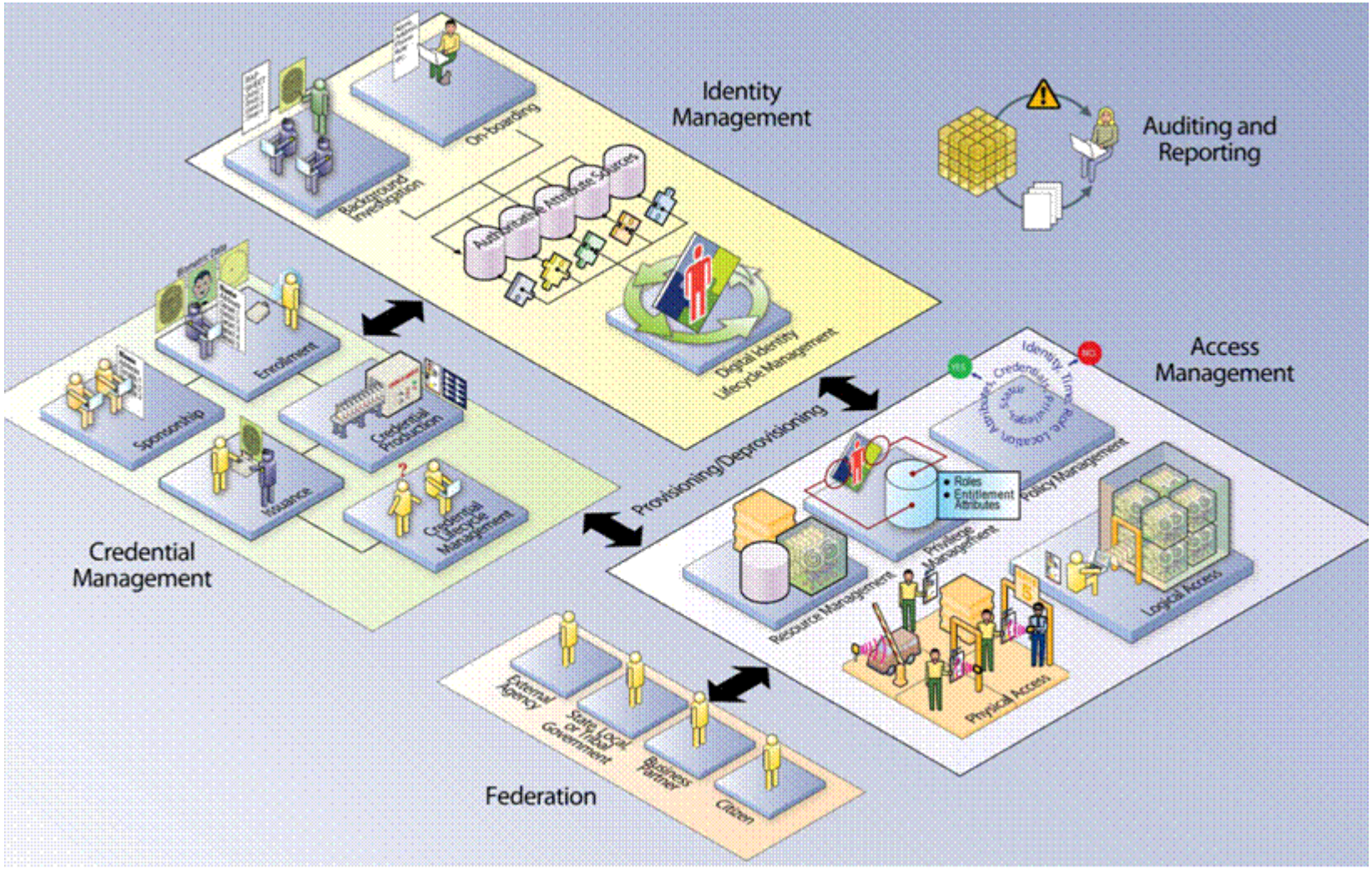


Figure 5: Example of PIV Credentialing Process

Note: The following section was extracted from the NIST publication, Federal Information Processing Standard Publication 201 (FIPS 201-2), "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013, and CIO Council Identity, Credential and Access Management Subcommittee (ICAMSC) document, "Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance v2."[33]

FIPS 201 defines the security requirements for processes that are part of the card issuance and management subsystem for a PIV system implementation. Additional security requirements are also imposed for issuance and management of the logical credentials supported by the PIV Card. Technical specifications for the implementation of the PIV system are described in detail in FIPS 201 Section 4, NIST SP 800-73, and NIST SP 800-76.

The following sections describe requirements and processes for several key lifecycle activities:

- Creating a new PIV record and issuing a new PIV Card
- Maintaining an existing PIV record and card
- Managing PIV keys

NOTE: The CIO Council Identity, Credential and Access Management Subcommittee (ICAMSC) document, "Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance v2" and FIPS 201-2 are not currently harmonized. As such, FIPS 201-2 shall take precedence over all guidance documents.

6.1 Creating a New PIV Record and Issuing a New PIV Card

The FICAM Roadmap and Implementation Guidance document defines the high-level process flow and steps for creating and issuing a PIV credential to a federal employee or contractor. The major process steps are as follows.

FIPS 201 requires the adoption and use of an approved identity proofing and registration process.

The following is an example process from the "FICAM Roadmap and Implementation Guidance" document.

6.1.1 Sponsorship

1. The applicant requests a PIV Card.
2. The sponsor substantiates the applicant‘s need for a PIV credential within the agency and authorizes the request for a PIV Card.
3. The sponsor enters basic information about the applicant into the PIV identity management system (IDMS), either on an individual basis, or as part of a group in a batched process. (Batch processing may be handled in various ways at individual agencies.)
4. The sponsor approves and digitally signs the applicant(s) PIV IDMS record(s).

6.1.2 Enrollment

1. The applicant appears for enrollment with supporting documentation. (Two forms of ID are required that meet FIPS 201-2 identity proofing requirements, at least one of which must be a government-issued photo ID.)

[33] "Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance," Version 2.0 December 2011, Identity, Credential and Access Management Subcommittee (ICAMSC), Federal CIO Council, can be found on the http://www.idmanagement.gov/ Web Site by searching the document FICAM_Roadmap_and_Implementation_Guidance_v2.

2. The registrar/enrollment official inspects and confirms all supporting documents using automated means if available. Registrar/enrollment official may also scan and retain a copy of all supporting documents.
3. The registrar/enrollment official establishes that the individual present matches the supporting documents.
4. The registrar/enrollment official confirms sponsor approval for PIV.
5. The registrar/enrollment official captures the applicant‘s digital facial image.
6. The registrar/enrollment official captures fingerprint biometrics from the applicant, typically both rolled and flat prints of all ten fingers. (These fingerprints are intended to be forwarded for the background investigation.)
7. The registrar/enrollment official captures any additional required biographic data from the applicant that was not captured during sponsorship.
8. The registrar/enrollment official digitally signs and submits the completed electronic enrollment package to the IDMS for storage and processing.
9. The IDMS verifies the integrity of that package by confirming completeness, accuracy, and digital signatures.

6.1.3 Adjudication

1. The IDMS may perform a 1-to-many search to assure that the individual identified in the package has not applied previously under a different name.
2. The adjudicator may receive notification that the enrollment package has been completed for the Applicant and requires a determination of eligibility to receive a PIV Card.
3. The adjudicator provides an initial interim card issuance determination based on fingerprint result findings and National Agency Check (NAC) results or a single final eligibility determination through a background investigation. At a minimum, FIPS 201 and OMB Memorandum M-05-24[34] require that the FBI National Criminal History Check (fingerprint check) be completed before credential issuance. FIPS 201 requires that identity credentials issued to individuals without a completed NACI or equivalent must be electronically distinguishable from identity credentials issued to individuals who have a completed investigation.
4. Full background check information is typically collected via related background investigation processes associated with on-boarding. The adjudicator provides a final card issuance determination based upon the results of the completed background investigation. If a card has been issued based upon the fingerprint check, and the investigation produces an unfavorable determination, the card should be revoked.
5. After a favorable fingerprint check result, the adjudicator approves card production for the credential on an interim (6 month) basis. This process may be automated based on integration with FBI results.
6. After a favorable adjudication result, the interim approval status is updated in the IDMS and on the PIV credential through an update to the NACI Indicator to show full approval. (The NACI Indicator is located on the PIV Authentication Certificate.) This process is handled different by many agencies.

[34] "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," OMB Memorandum M-05-24, August 5, 2005, http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf

6.1.4 Issuance

FIPS 201 requires the adoption and use of an approved issuance and maintenance process. An employee or contractor may be issued a PIV Card and logical credentials while a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or national security community investigation required for Federal employment is pending. The following is an example process from the "FICAM Roadmap and Implementation Guidance" document.

1. Depending on the issuance model, card stock or cards that have been pre-personalized with personal information are shipped and tracked to an issuance site.
2. The IDMS or the issuer notifies the applicant to schedule an issuance session.
3. Upon arrival, FIPS 201 requires that the issuer verify the applicant biometrically by performing a one-to-one match between the applicant and the fingerprint sample collected during enrollment or in the case a biometric match is not possible using an exception mechanism approved by the issuer.
4. The applicant's card is finalized, with any remaining personal information loaded on the chip. In the case of local printing, blank card stock is personalized, printed and finalized.
5. The applicant creates a PIN that will be used to gain access to the card certificates.
6. The certificates and PIN are loaded onto the credential (if they have not been so already) and the card is released to the cardholder.
7. The cardholder signs an agreement indicating acceptance of the terms and conditions of holding digital certificates. This is either a paper or electronic process.

6.2 Maintaining an Existing PIV Record and Card

The data and credentials held by the PIV Card may need to be invalidated prior to the expiration date of the card. The cardholder may retire, change jobs, or terminates employment, thus requiring invalidation of a previously active card. The card may be damaged, lost, or stolen, thus requiring a replacement. The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card management.

Maintenance activities are performed during various stages of the PIV lifecycle. The following is an example process from the "FICAM Roadmap and Implementation Guidance" document. Not all activities are performed for each PIV Card, and the activities listed below may not be performed in this order.

6.2.1.1 PIV Card Certificate Update

1. Cardholder is notified via automated system that PKI certificates held in the PIV Card are due to expire.
2. Cardholder follows directions in notification to request new certificates.
3. Automated system uses old certificate challenge/response to determine validity of renewal request and updates the certificates on the card.

6.2.1.2 Reissuance of PIV Card (Lost, Stolen, Compromised)

FIPS 201 specifies that, in case of reissuance, the entire registration and issuance process, including fingerprint and facial image capture, must be conducted. The card issuer verifies that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.

A cardholder applies for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of an employee status or attribute change or if one or more logical credentials have been compromised.

FIPS 201 recommends that the old PIV Card, if available, be collected and destroyed. FIPS 201 specifies that, if the card cannot be collected, normal operational procedures must be completed within 18 hours of notification. In some cases, 18 hours is an unacceptable delay. In that case, emergency procedures must be executed to disseminate this information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.

The following is an example process from the "FICAM Roadmap and Implementation Guidance" document.

1. Cardholder notifies an appropriate authority (agency specific, but could be security personnel, issuer, sponsor or other entity) that the PIV Card has been lost, stolen, or suffered compromise and is directed to an enrollment station for reissuance. (Wait times or additional security procedures may be required by agency policy for lost or stolen PIV Cards.)
2. The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) Federal Agency Smart Credential Number (FASC-N) values must be updated to reflect the change in status[35].
3. The CA is informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies will revoke certificates corresponding to the optional digital signature and key management keys if they have also been issued. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers within 18 hours of revocation.
4. Online Certificate Status Protocol (OCSP) responders are updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).
5. The entire registration and issuance process, including fingerprint and facial image capture, must be conducted.
6. The issuer verifies that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.
7. The issuer issues a new credential (following the procedures for initial issuance) and updates the IDMS record.
8. The issuer digitally signs the recaptured biometric sample and new credential record.
9. If issued, a new key management key is to be escrowed. Existing key management keys previously escrowed may be recovered in accordance with agency policy.

6.2.1.3 Renewal of PIV Card

Renewal is the process by which a PIV Card is replaced without the need to repeat the full registration procedure. The card issuer must verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials to current employees, the NACI checks are to be followed in accordance with the OPM guidance.

The PIV Card is valid for no more than six years but agencies may decide to have a shorter validity period of the card (e.g., three year card life aligned on the certificates). A cardholder is allowed to apply for a

[35] If the system is using the GUID instead of the FACS-N as the card identifier, it is the GUID which shall be updated in the data base.

renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card[36]. The card issuer will verify the cardholder's identity against the biometric information stored on the expiring card. The expired PIV Card must be collected and destroyed.

The same biometric data may be reused with the new PIV Card while the digital signature must be recomputed with the new FASC-N and the new PIV Card UUID.

The expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card. Hence, a new PIV authentication key and certificate must be generated. If the PIV Card supports the optional key management key, that key may be imported to the new PIV Card.

The following is an example process from the "FICAM Roadmap and Implementation Guidance" document.

1. The cardholder receives notice (automated or manual) within six weeks of PIV Card expiration.
2. The cardholder presents the current PIV Card to the registrar/enrollment official prior to the date of expiration.
3. The registrar/enrollment official ensures that the IDMS record for this individual states the credential is not expired. If the PIV Card presented is past the expiration date, the issuer must follow re-issuance procedures.
4. The registrar/enrollment official verifies the cardholder against the IDMS record digital photograph.
5. If the digital photograph and biometric reference data are stored locally within the IDMS, the same biometric data may be re-used for the new PIV Card. The same data may only be used if it accurately depicts the physical appearance of the applicant. If the photo and biometric data are not stored locally, the registrar/enrollment official recaptures biometrics and digital facial image.
6. The registrar/enrollment official submits all paperwork to the adjudicator or the IDMS for storage and processing.
7. The adjudicator verifies that the background investigation on record for the cardholder is still current and valid and approves issuance.
8. The issuer issues a new credential (following procedures for initial issuance) and updates the IDMS record.
9. The issuer digitally signs the recaptured biometrics and new credential record.
10. The new key management key is escrowed.

NOTE: FIPS 201-2 has changed some of these requirements and takes precedence. See FIPS 201-2 Section 2.9.1 PIV Card Reissuance Requirements.

6.2.1.4 PIN Change (Cardholder Requires or Requests New PIN)

The PIN on a PIV Card may need to be reset if the contents of the card are locked resulting from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency. PIN resets may be performed by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer must ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card. Departments and agencies may adopt more stringent procedures for PIN reset (including disallowing PIN reset, and requiring the termination of PIV Cards that have been locked); such procedures must be formally documented by each department and agency.

[36] Past the card expiration date, the FICAM guidance document requires the process to be a complete re-issuance procedure.

The following is an example process from the "FICAM Roadmap and Implementation Guidance" document.

1. The cardholder arrives at a designated support kiosk, approved computer terminal, issuance or enrollment station and puts the PIV Card into the reader.
2. The PIV system prompts the cardholder for his previous PIN (in cases where the PIN has not been forgotten).
3. If authentication is successful, the Cardholder selects PIN change.
4. For PIN change, the IDMS prompts the cardholder to enter the current PIN, enter a new PIN value and confirm the new PIN[37]. The system verifies that the entered PIN conforms to established policy for PIN values.
5. The system confirms that the PIN change was successful.

6.2.1.5 PIN Reset (PIN Is Blocked or Forgotten)

1. The cardholder arrives at a designated issuance or enrollment station and puts the PIV Card into the reader.
2. A biometric match between the cardholder and IDMS is required in order to request a new PIN.
3. The PIV system prompts the cardholder to enter a new PIN.
4. The system verifies that the entered PIN conforms to established policy for PIN values.
5. The system confirms PIN change was successful.

6.2.1.6 Card Termination

The termination process is used to permanently destroy or invalidate the use of the card, including the data and the keys on it, such that it cannot be used again. FIPS 201 specifies that the PIV Card be terminated under the following circumstances:

- An employee separates (voluntarily or involuntarily) from Federal service.
- An employee separates (voluntarily or involuntarily) from a Federal contractor.
- A contractor changes positions and no longer needs access to Federal buildings or systems.
- A cardholder is determined to hold a fraudulent identity.
- A cardholder passes away.

Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following:

- The PIV Card is collected and destroyed.
- The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N (and/or GUID) values must be updated to reflect the change in status.
- The CA must be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued must include the appropriate certificate serial numbers.

[37] The IDMS may verify the PIN has a correct length as well as a correct format and sends the command for the card to update the PIN value, but the IDMS should never store the cardholder PIN. The PIV Card will reject the proposed PIN if its length is not between 6 and 8 bytes.

- OCSP responders must be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).
- The personal information in identifiable form (IIF) that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.

6.3 Managing PIV Keys

PIV Cards will have one or more asymmetric private keys. To manage the public keys associated with the asymmetric private keys, departments and agencies are required to issue and manage X.509 public key certificates.

6.3.1.1 Architecture

FIPS 201 specifies that the CA that issues certificates to support PIV Card authentication participates in the hierarchical PKI for the Common Policy managed by the Federal PKI.

6.3.1.2 PKI Certificate

FIPS 201 specifies that all certificates issued to support PIV Card authentication be issued under the id-CommonHW policy and the id-CommonAuth policy as defined in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (COMMON)[38]. These requirements cover identity proofing and the management of CAs and registration authorities. CAs and registration authorities may be operated by departments and agencies, or outsourced to PKI service providers.

COMMON requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (i.e., the PIV Card). In addition, FIPS 201 requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.

COMMON specifies the use of RSA along with the key sizes and hash functions.

This standard allows additional cryptographic algorithms and key sizes as specified in the SP 800-78. Future enhancements to COMMON are expected to permit use of additional algorithms. PIV Card management systems are limited to algorithms and key sizes recognized by FIPS 201 and the current version of COMMON.

6.3.1.3 X.509 Certificate Contents

The required contents of X.509 certificates associated with PIV private keys are based on X.509 Certificate and CRL Profile for the Common Policy.[39]

6.3.1.4 X.509 CRL Contents

FIPS 201 specifies that CAs that issue certificates corresponding to PIV private keys issue CRLs every 18 hours, at a minimum.

6.3.1.5 PKI Repository and OCSP Responder(s)

The PIV PKI Repository and Online Certificate Status Protocol (OCSP) responder provides PIV Card and key status information across departments, agencies, and other organizations, to support high-assurance interagency PIV Card interoperation. Departments and agencies are responsible for notifying certificate

[38] "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework," Federal Public Key Infrastructure Policy Authority, http://www.idmanagement.gov/sites/default/files/documents/CommonPolicy.pdf

[39] "X.509 Certificate and CRL Profile for the Common Policy," Version 1.1, Federal Public Key Infrastructure Policy Authority, July 8, 2004

authorities (CA) when cards or certificates need to be revoked. CAs must maintain the status of servers and responders needed for PIV Card and certificate status checking.

FIPS 201 specifies that the expiration date of the authentication certificate not be after the expiration date of the PIV Card. If the card is revoked, the authentication certificate must be revoked. However, an authentication certificate (and its associated key pair) may be revoked without revoking the PIV Card and may then be replaced. The presence of a valid, unexpired, and unrevoked PIV authentication certificate on a card is proof that the card was issued and is not revoked.

Because an authentication certificate typically lasts several years, a certificate revocation mechanism is necessary. Two are conventional: the CRL and the OCSP. CAs that issue PIV authentication certificates must maintain a Lightweight Directory Access Protocol (LDAP) directory server that holds the CRLs for the certificates it issues, as well as any CA certificates needed to build a path to the Federal Bridge CA[40].

Certificates must contain the information needed to locate CRLs and the authoritative OCSP responder. In addition, every CA that issues PIV authentication certificates must operate an OCSP server that provides certificate status for every authentication certificate the CA issues.

6.3.1.6 Certificate and CRL Distribution

FIPS 201 requires distribution of CA certificates and CRLs using LDAP or Hypertext Transport Protocol (HTTP).[41]

PIV authentication certificates contain the FASC-N and the Card UUID (GUID) in the subject alternative name extension; hence, FIPS 201 specifies that these certificates not be distributed publicly via LDAP or HTTP. Individual departments and agencies can decide whether other user certificates (digital signature and key management) can be distributed via LDAP.

6.3.1.7 OCSP Status Responders

FIPS 201 specifies that OCSP[42] status responders be implemented as a supplementary certificate status mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued.

[40] The trend in most implementations, is to favor HTTP over LDAP

[41] Specific requirements are found in "Shared Service Provider Repository Service Requirements," http://www.idmanagement.gov/documents/shared-service-provider-repository-service-requirements w

[42] RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)," Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2560.txt

7 FIPS 201 and Biometrics[43]

The biometric data used during the PIV Card life cycle activities consists of the following:

- A full set of fingerprints used to perform law enforcement checks as part of the identity proofing and registration process
- An electronic facial image used for printing the facial image on the card as well as for performing visual authentication during card usage. A new facial image must be collected at the time of reissuance. The facial image is required to be stored on the card.
- Optionally:
  - Two different electronic fingerprints templates to be stored on the card for on-card-comparison during card usage.
  - One or two iris images.

All biometric data enumerated above are collected during the identity proofing and registration process. Implementation requirements for storage of biometric data on PIV Cards is dependent on use of specifications are contained in NIST SP 800-76.

FIPS 201 specifies that the two electronic fingerprints stored on the card and available for biometric terminal verification be accessible only over the contact interface and after the presentation of a valid PIN. Contactless access is permitted for the biometric data specified to be stored on the PIV Card only after the establishment of a Virtual Card Interface session under FIPS 201-2 and also requires a valid PIN to be presented to the card.

7.1 Biometric Data Collection, Storage, and Usage

The full set of fingerprints is collected from all PIV Card applicants who can provide them. The technical specifications for the collection and formatting of the ten fingerprints is contained in SP800-76. The fingerprints are used for one-to-many matching with the database of fingerprints maintained by the FBI. The fingerprints should be captured using FBI-certified scanners and transmitted using FBI standard transactions. This one-to-many matching is called biometric identification. The requirement for ten fingerprints is based on matching accuracy data obtained by NIST in large-scale trials and reported in NISTIR 7123.[44] Because biometric identification using fingerprints is the primary means for law enforcement checks, agencies must seek Office of Personnel Management (OPM) guidance for alternative means for performing law enforcement checks in cases where obtaining ten fingerprints is impossible.

A facial image is collected from all PIV applicants. The technical specifications for an electronic facial image are contained in SP800-76.

The electronic facial image:

- Shall be stored on the PIV Card as described in Section 4.2.3.1 of FIPS 201-2;
- Shall be printed on the PIV Card according to Section 4.1.4.1 of FISP 201-2;
- May be used for generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.6 of FISP 201-2; and
- May be used for automated facial authentication in operator-attended PIV issuance, reissuance, and verification data reset processes.

[43] Source: FIPS 201-2, page 44

[44] NISTIR 7123, "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, NIST, June 2004

- May also be used for authenticating PIV Cardholders covered under Section 508 of the Rehabilitation Act of 1973.

Two electronic fingerprints are collected from all PIV applicants, who can provide them, for storing on the card. Alternatively, these two electronic fingerprints can also be extracted from the ten fingerprints collected earlier for law enforcement checks. The technical specifications for the two electronic fingerprints are contained in SP800-76. The right and left index fingers are normally designated as the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary and secondary designations are taken from the following fingers, in decreasing order of priority:

1. Right thumb
2. Left thumb
3. Right middle finger
4. Left middle finger
5. Right ring finger
6. Left ring finger
7. Right little finger
8. Left little finger

The two mandatory fingerprints shall be used for preparation of templates to be stored on the PIV Card as described in Section 4.2.3.1 of FIPS 201-2. The fingerprints provide an interagency-interoperable authentication mechanism through a match-off-card scheme as described in Section 6.2.1 of FIPS 201-2. These fingerprints are also the primary means of authentication during PIV issuance and maintenance processes.

FIPS 201 specifies that these card fingerprints are used for one-to-one biometric verification against live samples collected from the PIV cardholder. Even though two fingerprints are available on the card, a department or agency has the option to use one or both of them for the purpose of PIV cardholder authentication. If only one fingerprint is used for authentication, then the primary finger is used first. In cases where there is difficulty in collecting even a single fingerprint of acceptable quality, the department or agency must perform authentication using the PIV authentication key with the PIN.

The optional fingerprints may be used for preparation of the fingerprint templates for on-card comparison as described in Section 4.2.3.1 of FIPS 201-2. OCC may be used to support card activation as described in Section 4.3.1 of FIPS 201-2. OCC may also be used for cardholder authentication (OCC-AUTH) as described in Section 6.2.2 of FIPS 201-2.

The electronic iris images may be stored on the PIV Card as described in Section 4.2.3.1 of FIPS 201-2. Agencies may choose to collect iris biometrics as a second biometric to support multimodal authentication to improve accuracy, operational suitability, to accommodate user preferences, or as a backup when the fingerprint biometric is unavailable.

FIPS 201 also requires that PIV biometric data is not readable by default and is protected through an authentication mechanism such as a PIN. An electromagnetically opaque sleeve or other technology is also required to protect against any unauthorized contactless access to personal or biometric information stored on a contactless IC.

7.2 Alternative Biometric Usage[45]

FIPS 201 restricts access by a terminal to the reference biometric fingerprint data stored on the PIV Card-application of the PIV Card. This restriction may prevent the efficient use of biometrics as an authentication mechanism in access control systems that require high throughput.

[45] Source: "Authentication Mechanisms for Physical Access Control," Smart Card Alliance Physical Access Council white paper, October 2009.

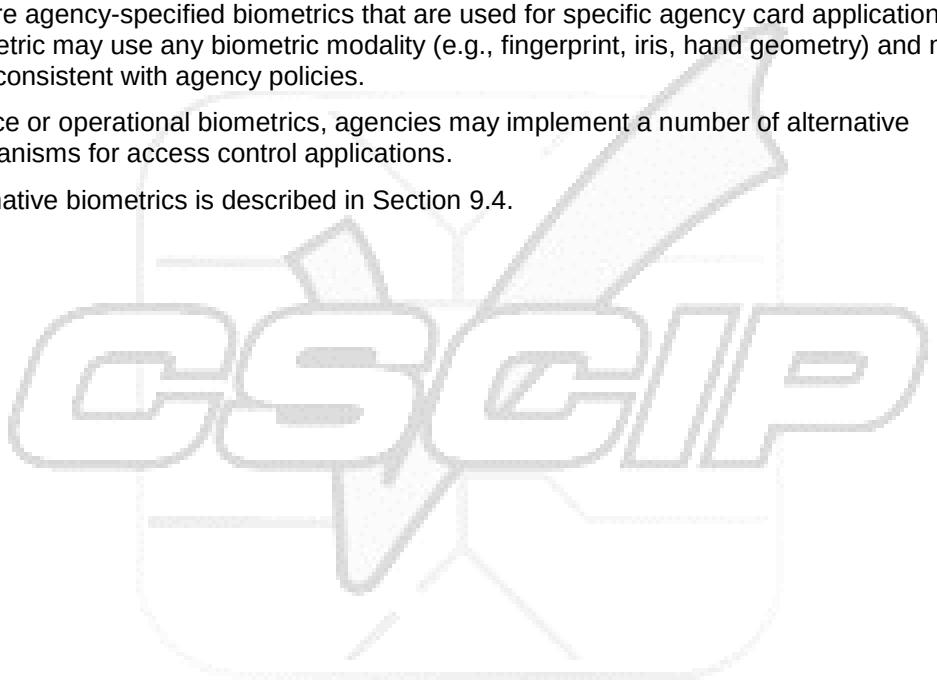
In FIPS 201, biometric matching to the reference biometric fingerprint templates stored on the PIV Card-application can only take place:

- After the PIV Card is inserted into a contact reader
  - And a PIN entered, allowing a terminal to do an off-card-comparison;
  - Or the On-Card-Comparison process is used.
- Or, after the PIV Card using the contactless interface has established a secure session using the Virtual Contact Interface protocol
  - And the PIN entered;
  - Or the On-Card-Comparison process is used.

However, FIPS 201 is silent about other card applications storing information, such as biometric templates, on the PIV Card chip or chips and accessed through both the contact and contactless interfaces, but provides no additional information on this topic. Agencies may use "operational biometrics," which are agency-specified biometrics that are used for specific agency card applications. An operational biometric may use any biometric modality (e.g., fingerprint, iris, hand geometry) and may be stored and used consistent with agency policies.

Using either reference or operational biometrics, agencies may implement a number of alternative authentication mechanisms for access control applications.

The use of the alternative biometrics is described in Section 9.4.



8 Authentication Levels

Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system. Guidance documents from OMB and NIST have defined assurance levels and authentication processes and technologies to be used for government-related electronic transactions requiring authentication. These guidelines form the basis for developing the authentication approaches for multiple government programs, including government-to-consumer, government-to-business, and government-to-government transactions.

8.1 OMB M-04-04

Note: The following section was extracted from OMB M04-04, "*E-Authentication Guidance for Federal Agencies,"*[46] *and NIST SP800-63, "Electronic Authentication Guideline."*[47]

OMB M04-04, "E-Authentication Guidance for Federal Agencies," describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has claimed an identifier (presented a credential[48] in this context) that refers to his or her identity. In this context, assurance is defined as 1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued. The four assurance levels are:

- Level 1: Little or no confidence in the asserted identity's validity. For example, Level 1 credentials allow people to bookmark items on a web page for future reference.
- Level 2: Some confidence in the asserted identity's validity. On balance, confidence exists that the asserted identity is accurate. Level 2 credentials are appropriate for a wide range of business with the public where agencies require an initial identity assertion (the details of which are verified independently prior to any Federal action).
- Level 3: High confidence in the asserted identity's validity. Level 3 is appropriate for transactions needing high confidence in the asserted identity's accuracy. People may use Level 3 credentials to access restricted web services without the need for additional identity assertion controls.
- Level 4: Very high confidence in the asserted identity's validity. Level 4 is appropriate for transactions needing very high confidence in the asserted identity's accuracy. Users may present Level 4 credentials to assert identity and gain access to highly restricted web resources, without the need for further identity assertion controls.

The OMB guidance defines the required level of authentication assurance in terms of the likely consequences of an authentication error. As the consequences of an authentication error become more serious, the required level of assurance increases. The OMB guidance provides agencies with the criteria for determining the level of E-authentication assurance required for specific applications and transactions, based on the risks and their likelihood of occurrence of each application or transaction.

OMB guidance outlines a 5 step process by which agencies should meet their E- authentication assurance requirements:

1. Conduct a risk assessment of the government system.

[46] "E-Authentication Guidance for Federal Agencies," OMB Memorandum M04-04, December 16, 2003, http://www.whitehouse.gov/OMB/memoranda/fy04/m04-04.pdf

[47] NIST Special Publication 800-63 (SP 800-63-2), "Electronic Authentication Guideline," August 2013, http://dx.doi.org/10.6028/NIST.SP.800-63-2

[48] OMB M04-04 defines a credential as: an object that is verified when presented to the verifier in an authentication transaction. SP 800-63-2 defines a credential as: An object or data structure that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a Subscriber.

2. Map identified risks to the appropriate assurance level.
3. Select technology based on E-authentication technical guidance.
4. Validate that the implemented system has met the required assurance level.
5. Periodically reassess the information system to determine technology refresh requirements.

To determine the appropriate level of assurance in the user's asserted identity, agencies must assess the potential risks, and identify measures to minimize their impact. Authentication errors with potentially worse consequences require higher levels of assurance. Business process, policy, and technology may help reduce risk. The risk from an authentication error is a function of two factors:

a) potential harm or impact, and

b) the *likelihood* of such harm or impact.

Categories of harm and impact include:

- Inconvenience, distress, or damage to standing or reputation
- Financial loss or agency liability
- Harm to agency programs or public interests
- Unauthorized release of sensitive information
- Personal safety
- Civil or criminal violations

Required assurance levels for electronic transactions are determined by assessing the potential impact of each of the above categories using the potential impact values described in Federal Information Processing Standard (FIPS) 199, "Standards for Security Categorization of Federal Information and Information Systems."[49] The three potential impact values are:

- Low impact
- Moderate impact
- High impact

The table below shows the mapping of the maximum potential impact to the four defined assurance levels.

	Assurance Level Impact Profiles			
Potential Impact Categories for Authentication Errors	**1**	**2**	**3**	**4**
Inconvenience, distress or damage to standing or reputation	Low	Mod	Mod	High
Financial loss or agency liability	Low	Mod	Mod	High
Harm to agency programs or public interests	N/A	Low	Mod	High
Unauthorized release of sensitive information	N/A	Low	Mod	High
Personal Safety	N/A	N/A	Low	Mod /High
Civil or criminal violations	N/A	Low	Mod	High

Table 5. Maximum Potential Impacts for each Assurance Level

[49] Federal Information Processing Standard 199 (FIPS 199), "Standards for Security Categorization of Federal Information and Information Systems," February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf

8.2 SP 800-63

Note: The following section was extracted from NIST SP800-63-2, "Electronic Authentication Guideline", August 2013.

NIST SP 800-63, "Electronic Authentication Guideline," provides guidelines for implementing the third step of the process defined in OMB M04-04, "Select the technology based on E-authentication technical guidance."

SP 800-63-2 defines three very important terms worth noticing which are copied below:

- **Attribute**: A claim of a named quality or characteristic inherent in or ascribed to someone or something.
- **Credential:** An object or data structure that authoritatively binds an identity (and optionally additional attributes) to a token possessed and controlled by a subscriber.
- **Token:** Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity.

As this section is based on SP 800-63, and these terms are not always defined the same way in other documents, it is important to keep in mind their meaning in this specific context.

After completing a risk assessment and mapping the identified risks to the required assurance level, agencies can select appropriate technology that, at a minimum, meets the technical requirements for the required level of assurance. In particular, SP 800-63 states specific technical requirements for each of the four levels of assurance in the following areas:

- Identity proofing and registration of applicants,
- Tokens (typically a cryptographic key or password) for proving identity,
- Token and credential management mechanisms used to establish and maintain token and credential information,
- Protocols used to support the authentication mechanism between the claimant and the verifier,
- Assertion mechanisms used to communicate the results of a remote authentication if these result.

A summary of the SP800-63 technical requirements for each of the four levels is provided below.

Level 1 - Although there is no identity proofing requirement at this level, the authentication mechanism provides some assurance that the same claimant is accessing the protected transaction or data. It allows a wide range of available authentication technologies to be employed and allows any of the token methods of Levels 2, 3, or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token.

Plaintext passwords or secrets are not transmitted across a network at Level 1. However this level does not require cryptographic methods that block offline attacks by an eavesdropper. For example, simple password challenge-response protocols are allowed.

In many cases an eavesdropper, having intercepted such a protocol exchange, will be able to find the password with a straightforward dictionary attack.

At Level 1, long-term shared authentication secrets may be revealed to verifiers. All assertions recognized within this guideline must indicate the assurance level of the initial authentication of the subscriber. At Level 1, assertions and assertion references must be protected from manufacture/modification and reuse attacks.

Level 2 – Level 2 provides single factor remote network authentication. At Level 2, identity proofing requirements are introduced, requiring presentation of identifying materials or information. A wide range of available authentication technologies can be employed at Level 2. For single factor authentication,

memorized secret tokens, pre-registered knowledge tokens, look-up secret tokens, out-of-band tokens, and single factor one-time password devices are allowed at Level 2. Level 2 also allows any of the token methods of Levels 3 or 4. Successful authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. Online guessing, replay, session hijacking and eavesdropping attacks are prevented. Protocols must also be at least weakly resistant to man-in-the middle attacks

Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated by the credentials service provider (CSP); however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. In addition to Level 1 requirements, assertions must be resistant to disclosure, redirection, capture and substitution attacks. Approved cryptographic techniques are required for all assertion protocols used at Level 2 and above.

Level 3 – Level 3 provides multi-factor remote network authentication. At least two authentication factors are required. At this level, identity proofing procedures require verification of identifying materials and information. Level 3 authentication is based on proof of possession of the allowed types of tokens through a cryptographic protocol. Multi-factor software cryptographic tokens are allowed at Level 3. Level 3 also allows any of the token methods of Level 4. Level 3 authentication requires cryptographic strength mechanisms that protect the primary authentication token against compromise by the protocol threats for all threats at Level 2 as well as verifier impersonation attacks. Various types of tokens may be used as described in Section 6 of SP 800-63-2.

Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. The claimant must first unlock the token with a password or biometric, or must use a secure multi-token authentication protocol to establish two-factor authentication (through proof of possession of a physical or software token in combination with some memorized secret knowledge). Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. In addition to Level 2 requirements, assertions shall be protected against repudiation by the verifier.

Level 4 – Level 4 is intended to provide the highest practical remote network authentication assurance. Level 4 authentication is based on proof of possession of a key through a cryptographic protocol. At this level, in-person identity proofing is required. Level 4 is similar to Level 3 except that only “hard” cryptographic tokens are allowed. The token is required to be a hardware cryptographic module validated at Federal Information Processing Standard (FIPS) 140-2 Level 2 or higher overall with at least FIPS 140-2 Level 3 physical security. Level 4 token requirements can be met by using the PIV authentication key of a FIPS 201 compliant PIV Card. Level 4 requires strong cryptographic authentication of all parties and all sensitive data transfers between the parties. Either public key or symmetric key technology may be used. Authentication requires that the claimant prove through a secure authentication protocol that he or she controls the token. All protocol threats at Level 3 shall be prevented at Level 4. Protocols must also be strongly resistant to man-in-the-middle attacks. Long-term shared authentication secrets, if used, are never revealed to any party except the claimant and verifiers operated directly by the CSP; however, session (temporary) shared secrets may be provided to independent verifiers by the CSP. Strong approved cryptographic techniques are used for all operations. All sensitive data transfers are cryptographically authenticated using keys bound to the authentication process.

At Level 4, bearer assertions[50] are not be used to establish the identity of the claimant to the relying party (RP). “Holder-of-key” assertions may be used, provided that the assertion contains a reference to a key that is possessed by the subscriber and is cryptographically linked to the Level 4 token used to authenticate to the verifier. The relying party should maintain records of the assertions it receives, to support detection of a compromised verifier impersonating the subscriber.

[50] See section 9 of SP 800-63-2 for more details about these assertions.

The following table lists the token types as defined by SP 800-63-2 (in section 6.1.2)

Token Name	Definition (CSP means Credential Service Provider)	Something you Have	Know	Are
Memorized Secret	A secret shared between the Subscriber and the CSP. Memorized Secret Tokens are typically character strings (e.g., passwords and passphrases) or numerical strings (e.g., PINs.)		√	
Pre-Registered Knowledge	A series of responses to a set of prompts or challenges. These responses may be thought of as a set of shared secrets.		√	
Look Up Secret Token	A physical or electronic token that stores a set of secrets shared between the Claimant and the CSP	√		
Out of Band Token	A physical token that is uniquely addressable and can receive a Verifier-selected secret for one-time use.	√		
Single Factor (SF) or One-Time Password (OTP)	A hardware device that supports the spontaneous generation of one-time passwords.	√		
Single Factor Cryptographic Device	A hardware device that performs cryptographic operations on input provided to the device.	√		
Multi-factor (MF) Software Cryptographic token[51]	A cryptographic key is stored on disk or some other "soft" media and requires activation through a second factor of authentication.	√	√(*) or √(*)	
Multi-factor (MF) One-Time Password (OTP) Device (*)	A hardware device that generates one-time passwords for use in authentication and which requires activation through a second factor of authentication.	√	√(*) or √(*)	
Multi-factor (MF) Cryptographic Device (*)	A hardware device that contains a protected cryptographic key that requires activation through a second authentication factor.	√	√(*) or √(*)	

Table 6. Token Types as Defined in SP 800-63-2

Document SP 800-63-2 shows in its Table 7 the various level of authentications which can be reached by combining different tokens described above.

Table 7 below shows a simplified approach to the token types that are allowed at each assurance level.

[51] (*) For this token, only one of the two activation factors is required: either what you know or what you have.

Table 7. Token Type by Assurance Level[52] [53]

	Assurance Level			
Allowed Token Types	**1**	**2**	**3**	**4**
Hard cryptographic token	√	√	√	√
Soft cryptographic token	√	√	√	
Zero knowledge password	√	√	√	
One-time password device	√	√	√	
Strong password	√	√		
PIN	√			

8.3 Authentication Levels, FIPS 201 and PIV

In the context of the PIV Card, identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV Card. The authenticated identity can then be used to determine the permissions or authorizations that are granted to that identity to access various physical and logical resources.

8.3.1 FIPS 201 Assurance Levels

Note: The following section was extracted from the NIST publication, Federal Information Processing Standard Publication 201 (FIPS 201-2), Personal Identity Verification (PIV) of Federal Employees and Contractors, Section 6-1, August 2013, pages 51-52

FIPS 201 defines four levels of assurance for identity authentication supported by the PIV Card application. Each assurance level sets a degree of confidence established in the identity of the holder of the PIV Card. The entity performing the authentication establishes confidence in the identity of the PIV Cardholder through the following:

1) The rigor of the identity proofing process conducted prior to issuing the PIV Card.
2) The security of the PIV Card issuance and maintenance processes; and
3) The strength of the technical mechanisms used to verify that the cardholder is the owner of the PIV Card.

Section 2 of FIPS 201-2 defines requirements for the identity proofing, registration, issuance, and maintenance processes for PIV Cards and establishes a common level of assurance in these processes. The PIV identity proofing, registration, issuance, and maintenance processes meet or exceed the requirements for E-Authentication Level 4 [OMB0404]. The PIV Card contains a number of visual and logical credentials. Depending on the specific PIV data used to authenticate the holder of the PIV Card to an entity that controls access to a resource, varying levels of assurance that the holder of the PIV Card is the owner of the card can be achieved. This is the basis for the following PIV assurance levels defined in the FISP 201-2 Standard:

- LITTLE or NO Confidence—Little or no assurance in the identity of the cardholder;
- SOME Confidence—A basic degree of assurance in the identity of the cardholder
- HIGH Confidence—A strong degree of assurance in the identity of the cardholder
- VERY HIGH Confidence—A very strong degree of assurance in the identity of the cardholder.

Parties responsible for controlling access to Federal resources (both physical and logical) determine the appropriate level of identity assurance required for access, based on the harm and impact to individuals

[52] "HSPD-12: Defining a Federal PKI Framework," Judith Spencer presentation, Smart Cards in Government Conference, April 2006

[53] See Table 6 (Token Requirements per Assurance level) in SP 800-63-2 for a complete description of these levels

and organizations as a result of errors in the authentication of the identity of the PIV Cardholder. Once the required level of assurance has been determined, the authentication mechanisms specified within this section may be applied to achieve the required degree of confidence in the identity of the PIV Cardholder.

The levels of identity authentication assurance defined within FIPS 201 are closely aligned with the discussion in OMB M-04-04.

Table 8 below shows the notional relationship between the PIV assurance levels and the OMB M04-04 assurance levels.

Table 8. Relationship between PIV and E-Authentication Assurance Levels[54]

PIV Assurance Levels	Comparable OMB E-Authentication Levels	
	Level Number	Description
LITTLE or NO confidence	Level 1	Little or no confidence in the asserted identity's validity
SOME confidence	Level 2	Some confidence in the asserted identity's validity
HIGH confidence	Level 3	High confidence in the asserted identity's validity
VERY HIGH confidence	Level 4	Very high confidence in the asserted identity's validity

8.3.2 PIV Authentication Mechanisms

Note: The following section was extracted from the NIST SP 800-73-4, Interfaces for Personal Identity Verification – Part 1: PIV Card Application Namespace, Data Model and Representation, Draft May 2014, Appendix B, pages 35-45.

FIPS 201 describes PIV authentication as the "process of establishing confidence in the identity of the cardholder presenting a PIV Card." The fundamental goal of using the PIV Card is to authenticate the identity of the cardholder to a system or person that is controlling access to a protected resource or facility. This end goal may be reached by various combinations of one or more of the validation steps described below:

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

- Visual inspection of the tamper-proofing and tamper-resistant features of the PIV Card as defined in FIPS 201;
- Use of cryptographic challenge-response schemes with symmetric keys; and
- Use of asymmetric authentication schemes to validate private keys embedded within the PIV card.

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

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

Cardholder Validation (HolderV) — This is the process of establishing that the PIV Card is in the

[54] This table is the copy of Table 6-1 from SP 800-63-2, page 52

possession of the individual to whom the card has been issued. Classically, identity authentication is achieved using one or more of these factors: a) something you have, b) something you know, and c) something you are. The assurance of the authentication process increases with the number of factors used. In the case of the PIV card, these three factors translate as follows: a) something you have – possession of a PIV card, b) something you know – knowledge of the PIN, and c) something you are – the visual characteristics of the cardholder, and the live fingerprint or iris image samples provided by the cardholder. Thus, mechanisms for PIV cardholder validation include:

- Presentation of a PIV Card by the cardholder;
- Matching the visual characteristics of the cardholder with the photo on the PIV card;
- Matching the PIN provided with the PIN on the PIV card; and
- Matching the live fingerprint samples provided by the cardholder with the biometric information embedded within the PIV card.

Table 9summarizes the types of validation activities that are included in each of the PIV authentication mechanisms.

Table 9. Summary of PIV Authentication Mechanisms from SP800-73

PIV Authentication Mechanism	Card Validation Steps (CardV)	Credential Validation Steps (CredV)	Cardholder Validation Steps (HolderV)
PIV Visual Authentication	Counterfeit, tamper, and forgery check	Expiration check	Possession of card Match of card visual characteristics with cardholder
PIV CHUID		Expiration check CHUID signature check	Possession of card
Symmetric Card Authentication Key	Perform challenge and response with a PIV symmetric key		Possession of card
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 Establishment	Establish Secure Messaging with card verifiable certificate	Certificate validation of a PIV certificate	Possession of card
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

PIV Authentication Mechanism	Card Validation Steps (CardV)	Credential Validation Steps (CredV)	Cardholder Validation Steps (HolderV)
PIV Biometric		Expiration check CHUID signature check (optional) PIV Biometric signature check (optional) Match CHUID FASC-N/GUID with PIV Biometric FASC-N/GUID	Possession of card Match PIN provided by cardholder Match cardholder biometric with PIV biometric
PIV Biometric (Attended)		Expiration check CHUID signature check PIV Bio signature check Match CHUID FASC-N/GUID with PIV Bio FASC-N/GUID	Possession of card Match PIN provided by cardholder Match of cardholder biometric to PIV biometric *in view of attendant*
On-Card Biometric Comparison	Establish Secure Messaging	Certificate validation of a PIV certificate	Possession of card Match OCC data provided by Cardholder

9 FIPS 201/PIV Card Use Cases: Physical Access

HSPD-12 explicitly requires the use of PIV cards "in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems." The PIV Card employs microprocessor-based smart card technology, and is designed to be counterfeit-resistant, tamper-resistant, and interoperable across Federal government facilities. Additionally, the FIPS 201 standards suite defines the authentication mechanisms for transactions between a PIV Card and a relying party. FIPS 201 does not, however, elaborate on the uses and applications of the PIV card.

The PIV Card may be used to authenticate the identity of the cardholder in a physical access control environment. For example, a Federal facility may have physical entry doors that have human guards at checkpoints, or may have electronic access control points. The PIV-supported authentication mechanisms for physical access control systems are summarized in Table 10. An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level. Moreover, the authentication mechanisms in the following table can be combined to achieve higher assurance levels[55].

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
LITTLE or NO confidence	VIS, CHUID
SOME confidence	PKI-CAK, SYM-CAK
HIGH confidence	BIO
VERY HIGH confidence	Bio-A,OCC-Auth, PKI-Auth

Table 10. Level of Assurance & PIV Authentication Mechanisms

For detailed information on how PIV/PIV-I cards can be used in physical access control systems, the document Personal Identity Verification in Enterprise Physical Access Control Systems V3 provides all the necessary details.[56]

> *Note: Sections 9.1 and 9.2 were extracted from document, "Federal Identity, Credential and Access Management Roadmap and Guidance," pages 103-110*

9.1 Current PACS

Agencies control access to their facilities through the use of PACS. Before HSPD-12 credentials, processes for granting physical access relied heavily on visual inspection and electronic access using diverse legacy technologies. Proximity cards using 125 kHz frequency and tokens were the predominant legacy technologies, but magnetic stripe, bar code, barium ferrite, and some contactless smart cards technologies were also used across the Federal government.[57] With the exception of some contactless smart cards, each of these technologies transmits a static number, which is matched against an access control list, to the PACS in order to grant access.

[55] Combinations of authentication mechanisms are specified in NIST Special Publication SP 800-116, "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)", http://csrc.nist.gov/publications/PubsSPs.html

[56] http://idmanagement.gov/sites/default/files/documents/Personal%20Identity%20Verification%20in%20Enterprise%20Physical%20Access%20Control%20Systems_v3_20140326.pdf

[57] Additional information on PACS technology can be found in CSCIP Module 5, "Smart Card Usage Models -- Identity and Security," Section 5.

Legacy PACS implementations provide little assurance in the identity of the individual requesting access. Transmission rates for the technologies are relatively low, which limits the size of the number that can be transmitted. The small number size combined with the prevalence of proprietary formats increases the chances that a card number will not be unique, which could allow an unintended individual access. Additional authentication factors that could increase assurance, such as PINs and biometrics, are not widely used outside of highly secured facilities.

PACS are commonly comprised of readers located at a doorway or portal, and locking devices installed at access points throughout a facility. One or more servers store identity, card, access point, and transaction information. To improve the speed of the access control transaction and reduce single points of failure, information is distributed to an array of panels that receive information from the readers, make access control decisions and release locking devices based on predefined rules. The PACS panels are normally located in the secured zones of the building.

The FICAM guidance document identifies the following challenges in the current use of PACS:

- **Interoperability.** PACS deployed in many Federal buildings are generally facility-centric rather than enterprise-centric and utilize proprietary PACS architectures. Therefore, many issued ID cards operate only with the PACS for which they were issued.
- **Scalability.** Some deployed systems are limited in their capability to process the longer credential numbers (i.e., CHUID, GUID and FASC-N) associated with PIV cards necessary for government-wide interoperability.
- **Security.** Deployed PACS readers can read an identifying number from a card, but in most cases they do not perform a cryptographic challenge/response exchange. Most bar code, magnetic stripe, and contact cards can be copied easily. The technologies used in these systems may offer little or no identity assurance (i.e., they validate the card not the cardholder).
- **Validity.** Many existing PACS verify expiration of credentials through a date stored in a site database. There is no simple way to synchronize the expiration or revocation of credentials for a Federal employee or contractor across multiple sites.

It should be noted the E-PACS document [58] uses the term “efficiency” instead of “interoperability” in its list of challenges:

- **Efficiency**. Use se of PACS personal identification numbers (PINs), public key infrastructure (PKI), and biometrics (BIO) with deployed PACS is managed on a site-specific basis. Individuals must enroll PACS PINs, keys, and biometrics at each site. Since PACS PINs, keys, and biometrics are often stored in a site database, they may not be technically interoperable with PACS at other sites.

9.2 FICAM Roadmap: Target PIV Card Use with PACS[59]

The FICAM guidance document defines the following target use case for full implementation of the PIV Card for electronic physical access for employees and contractors based on the guidance provided in SP 800-116 and technically detailed in the document “Personal Identity Verification in Enterprise Physical Access Control Systems V3.” By establishing an access control enterprise, agencies promote government-wide interoperability and resolve the security challenges in the current state. Multi-factor authentication involves three distinct types of authentication factors:

a) Something you have, in this case, a PIV card,

b) Something you know, knowledge of the PIN to access protected areas of the PIV card, and

c) Something you are, cardholder fingerprint match with biometric data stored on the card.”

[58] Personal Identity Verification in Enterprise Physical Access Control Systems_v3_20140326.pdf
[59] Source: FICAM Roadmap and Guidance.

Note: The following section is extracted from the PIV in Enterprise PACS V3.pdf document (Section 4). The notion of OCC-Auth is not mentioned in this section as the document has not been updated yet incorporated this new notion from FIPS 201-2. OCC-Auth is a "who you are" factor and the PIN presentation is a "what you know factor".

9.2.1 Smart Card Authentication Mechanisms

PIV and PIV-I cards contain four electronic identification and authentication mechanisms, which alone or in conjunction with other authentication mechanisms can establish confidence (to varying levels of assurance) in the identity of the cardholder:

- **PIV Authentication Certificate (PKI-Auth)** allowing PKI-based authentication only accessible via the contact interface when the user PIN is provided.
- **Biometric (BIO or BIO-A, if attended)** authentication of the cardholder's fingerprints or the optional iris images using biometric templates on the card, including verification of the signature and signer.
- **Cardholder Unique Identifier (CHUID)[60],** with contact or contactless read of the CHUID object, including verification of the signature and signer.
- **Card Authentication Key (PKI-CAK),** allowing cryptographic authentication of the card via the contact or contactless interface. This is a mandatory certificate on PIV[21] and PIV-I cards. CAK may also have an addition optional symmetric key on PIV Cards.[22]
- **Secure Messaging Authentication (SM-Auth),** with contact or contactless interface. SM-Auth uses the optional Secure Messaging Key to create a secure session (confidentiality and integrity) between the PIV Card and the application. SM-Auth provides card authentication as well, as the card uses a private-public key pair which can be verified using its associated certificate.

[FIPS 201] and [NIST SP 800-116] offer detailed information in regards to authentication mechanisms and levels of confidence. This document leverages information from [FIPS 201] and builds upon guidance from [NIST SP 800-116] for PACS.

Notes:

1. *The PIV/PIV-I PIN is required to be presented to the card when BIO, BIO-A or PKI-Auth mechanisms are used. The PIN is considered as a factor (what you know) only when the PACS has active cryptographic proof that it can trust the card to which the PIN was presented (CAK, PKI-Auth) and the BIO information comes from that same card.*
2. *In the following table, OCC-Auth is not indicated. When the card had a cryptographic proof of a good OCC, it is equivalent to a Bio or Bio(A) but without the PIN being presented to the card (so one factor less)*

PIV Authentication Mechanism	What You Have	What You Know	Who You Are	# of Factors	Interface
PKI-Auth + BIO-A	Smart card with crypto key (High Assurance)	PIN with crypto proof (Medium Assurance)	Observed fingerprint or iris (Medium Assurance)	3	Contact
PKI-Auth + BIO	Smart card with crypto key (High Assurance)	PIN with crypto proof (Medium Assurance)	Fingerprint or iris (Low Assurance)	3	Contact

[60] When used alone, CHUID verification is not considered an authentication method by FIPS 201-2. It must be combined with another method such as a visual verification of the card (VIS).

PIV Authentication Mechanism	What You Have	What You Know	Who You Are	# of Factors	Interface
CAK or SM + BIO-A	Smart card with crypto key (High Assurance)	PIN with indirect verification assumption (Low Assurance)	Observed fingerprint or iris (Medium Assurance)	3	Contact
CAK or SM + BIO	Smart card with crypto key (High Assurance)	PIN with indirect verification assumption (Low Assurance)	Fingerprint or iris (Low Assurance)	3	Contact
BIO-A	Card (Low Assurance)		Observed fingerprint or iris (Medium Assurance)	2	Contact
PKI-Auth	Smart card with crypto key (High Assurance)	PIN with crypto proof (Medium Assurance)		2	Contact
BIO			Fingerprint or iris (Low Assurance)	1	Contact
CAK or SM	Smart card with crypto key (High Assurance)			1	Contact/ Contactless
CHUID + VIS	Printed security feature on the PIV Card (Low Assurance)			1	Contact/ Contactless

Table 11. PIV Authentication Mechanisms and Factors

For PIV and PIV-I cards, the authentication mechanisms are defined as follows (see Section 8 of "PIV in Enterprise PACS v3" for more discussion):

A. **VIS**: Visual authentication entails inspection of the topographical features on the front and back of the PIV or PIV-I card. The human guard checks to see that the PIV or PIV-I card looks genuine, compares the cardholder's facial features with the picture on the card, checks the expiration date printed on the card, verifies the correctness of other data elements printed on the card, and visually verifies the security feature(s) on the card. The effectiveness of this mechanism depends on training, skill, and diligence of the guard (e.g., to match the face in spite of changes in beard, mustache, hair coloring, eye glasses).

B. **CHUID + VIS:** The controller/panel controlling access to the door receives frequent updates from the PACS server and validates the CHUID on the PIV or PIV-I card. In order to achieve single factor authentication, the asymmetric signature of the CHUID must also be validated.

C. **CAK (or SM):** Authentication of card is completed using the CAK (or the SM-Auth key), a unique cryptographic key that may be used on a contactless or contact card in a challenge/response protocol. The PACS obtains the CAK certificate from the PIV or PIV-I card, validates the certificate (check the certificate's expiration date, signature validation, revocation status) and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate. The certificate and rights to access the facility are provisioned in the PACS. For example, when the symmetric CAK is present and used (non-interoperable mechanism), the card reader obtains the diversification element from the card, calculates the card diversified key, and uses the key in a challenge/response to verify the card is authentic. The establishment of a Secure Messaging session (SM-Auth) provides card authentication as well.

D. **BIO:** The PIN is presented to the card allowing the reader to read the reference biometric information and to attempt a match with the live sample. The cardholder provides a live fingerprint or an optional iris biometric sample, which is validated against the biometric information embedded within the PIV or PIV-I card. The PACS verifies the signature on the biometric data object. This authentication mechanism does not include authentication of the PIV or PIV-I card.

E. **BIO-A:** Biometric authentication performed in the presence of a human guard is called BIO-A. The PIN is presented to the card allowing the reader to read the reference biometric information and to attempt a match with the live sample. In addition to the steps in process D, a security officer supervises the use of the PIV or PIV-I card and the submission of the PIN and the biometric sample by the cardholder.

F. **PKI-Auth:** The cardholder provides the PIN for validation by the PIV or PIV-I card. The PIV or PIV-I card validates the PIN allowing use of the PKI-Auth Key. The PACS validates the certificate (check the certificate's expiration date, signature validation, revocation status) and sends a challenge to the card to verify that the card holds the private key corresponding to the certificate. As a result of the successful cryptographic challenge/response, the successful PIN presentation is confirmed to the PACS.

G. **CAK (or SM) + BIO:** This includes an integration of the steps from options C and D. The verification of the PIN can be trusted because the PIV or PIV-I card is authenticated by the CAK (or SM).

H. **CAK (or SM) + BIO-A:** This includes an integration of the steps from options C and E. The verification of the PIN can be trusted because the PIV or PIV-I card is authenticated by the CAK (or SM).

I. **Card PIN**: The presentation of the PIN to the card is not considered a factor by the PACS unless the PACS can validate that the card is a valid PIV or PIV-I card. As such, it does not appear in the table as an independent mechanism. There are only two basic mechanisms for determining that a card is a valid PIV or PIV-I card, and both use cryptographic challenge/response:

    a. CAK or SM, which does not require a PIN but indicates the card can be trusted; and

    b. PKI-Auth, which requires the correct PIN for the card to execute the authentication.

9.3 Selection of Authentication Mechanisms

Note: This section was extracted from SP800-116.

Since the areas accessible via different access points within a facility do not all have the same security requirement, the PIV authentication mechanisms should be selected to be consistent with, and integral to, the overall security requirements of the protected area. A given facility may need multiple authentication mechanisms. Therefore, the designation of "Controlled, Limited, Exclusion" areas, is applied to the protected area. Specifically, SP 800-116 recommends PIV authentication mechanisms for "Controlled, Limited, Exclusion" in terms of authentication factors as shown in Table 12.

Table 12. Authentication Factors for Security Areas from SP 800-116

Security Areas	Number of Authentication Factors Required
Controlled	1
Limited	2
Exclusion	3

PIV authentication mechanisms should be implemented in accordance with Table 12. **Error! Reference source not found.** illustrates the innermost perimeter at which each PIV authentication mechanism may be used based on the authentication assurance level of the mechanism. The combined effect of Table 12 and **Error! Reference source not found.** determines exactly what mechanisms may be used. An xhaustive list of possible uses of PIV authentication mechanisms against protected areas is provided in Appendix C of SP800-116.

Visual (VIS), Cardholder Unique Identifier (CHUID), Biometric (BIO), Attended Biometric (BIO-A), and PIV Authentication Key (PKI) are PIV authentication mechanisms defined in FIPS 201. Card Authentication Key (CAK) is an optional PIV authentication mechanism.

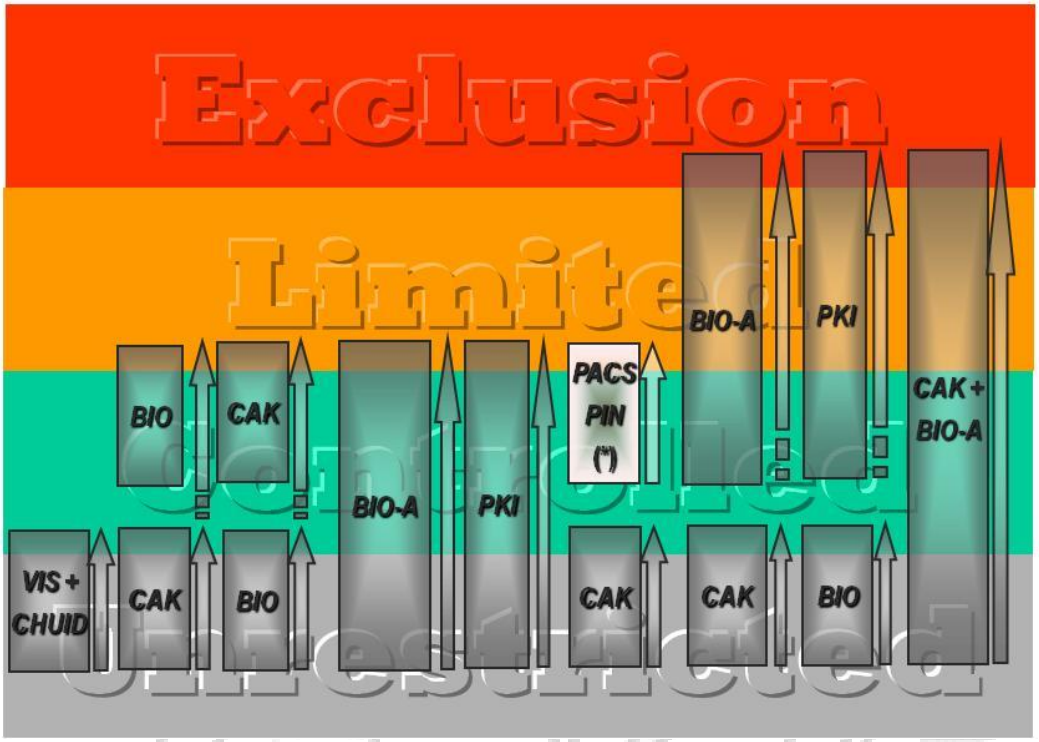


Figure 6. Use of PIV Authentication Mechanisms by Security Area based on SP800-116

9.4 Alternative Authentication Mechanisms using the PIV Card

The following sections describe multiple authentication mechanisms that could be used to address agency-specific requirements. The mechanisms incorporate a mutual authentication protocol (MAP), mutual registration, and widely-deployed mechanisms such as combinations of cards, PINs, and biometric factors. Before any data such as biometric templates or PINs are transmitted, techniques can be used to authenticate the data, card and reader and to ensure the confidentiality of the exchange. The mechanisms discussed in this section are not currently described in the PIV specification.

9.4.1 Operational Biometrics with Enrollment on System and Match on System

FIPS 201 restricts access to the reference biometric fingerprint data stored on the PIV Card This restriction may prevent the efficient use of biometrics as an authentication mechanism in access control systems that require high throughput. In FIPS 201, biometric matching to the reference biometric fingerprint templates stored on the PIV Card can only take place after the PIV Card is inserted into a contact reader (or a contactless reader with a Virtual Contact Interface established) and a PIN entered.

An agency that wants to implement biometrics for physical access using the contactless interface without an additional requirement for PIN entry should consider using operational biometrics. Using operational biometrics, an agency will enroll biometric data separately and store data in an agency-specific data repository (e.g., PACS server, control panel, or reader). The FASC-N (or GUID) read from the contactless PIV Card acts as a reference pointer to the specific biometric data to be matched for user

authentication. Matching can take place at the PACS server, control panel, or reader. The biometric data can be stored in a different location than the location where the matching takes place.

In an operational biometric implementation, any biometric technology can be used, including fingerprint, iris, face, vein, or hand geometry. Interoperability among agencies is achieved during PACS registration when the reference fingerprint biometric can be matched after the PIV Card is read and the PIN entered. Enrollment of the operational biometric can be as simple as copying the reference biometric fingerprint templates to the local PACS server or conducting a separate biometric enrollment immediately following PACS registration. The person is enrolled in the PACS database and the person's biometric information is captured and stored, indexed by either an identifier that is assigned by the PACS itself or an external identifier that the person presents at the time of verification (e.g., FASC-N or GUID from the PIV card).

This method provides one-factor authentication when an index value on the PIV Card (FASC-N or GUID) is used to find the reference biometric in the PACS database (since the card is not authenticated). The fact that the identifier comes from a card can sometimes be considered to be a second authentication factor (what you have). However, since the card is not authenticated, considering this a second factor opens the risk of successfully authenticating a counterfeit card.

When biometric verification is attended (i.e., the card is visually verified by an attendant), the second factor (what you have), while not electronically verified, exists—the features printed on the card are verified by the attendant. This method provides two authentication factors when used in conjunction with card authentication: what you have (the card) and match-on-system biometric verification that the cardholder is who the cardholder claims to be (who you are).

This mode is called CHUID + BIO to PACS in the "PIV in Enterprise PACS v3" document and is described in detail in its section 10.2.11 (Pattern # 12)

9.4.2 Reference Biometric with Match on System and Contactless Read of Encrypted Biometric Template on Card

Another alternative to the FIPS 201 requirement for PIN entry and contact read of the reference biometric is to define a separate, agency-specific application that is resident in the memory of the PIV Card and co-located with the FIPS 201-compliant PIV application. To ensure agency interoperability, each of the two card applications can be independently accessed by a reader by selecting the appropriate application identifier. The agency-specific application can define a different protocol that permits contactless reading of the reference biometric fingerprint template without requiring PIN entry.

To protect personal privacy when transferring data from the card to the reader over the contactless interface, the fingerprint templates stored in the agency-specific application would be encrypted. Decryption of the fingerprint templates could be accomplished through the use of a symmetric key (privacy key), generated during card production and unique to each card. The privacy key may be stored in a separate, non-PIV applet so that it may only be accessed through the contact interface or by reading the magnetic stripe.

This approach to contactless biometric reading presents some unique challenges for the PACS. If the encrypted biometric templates are to be read from the card through the contactless interface, the reader must have some way of first obtaining the privacy key. This requirement can be met by configuring the reader to include a magnetic stripe reader and swiping the card before presenting the card to the contactless interface. As an alternative, the privacy key can be stored at the reader or PACS server following a one-time local PACS registration process. This approach is currently implemented by the Transportation Worker Identification Credential (TWIC) program described in Section 15.2.

9.4.3 Operational Biometric with Enrollment on Card and Match on Card

The approach described as operational biometric with enrollment on card and match on card is identical to the OCC technique now allowed by FIPS 201-2. However, with the use of operational biometrics,

instead of using a standard reference fingerprint biometric, any biometric technology can be used, including a proprietary fingerprint or any iris, face, vein, or hand geometry technology.

This method would require the following:

- An available container on the card[61] (possibly for each PACS) in which to store the operational biometric
- Secure communication between the card and the PACS (or at least between the card and the biometric reader), preventing the cardholder's biometric template from being exposed during contactless communication
- Mutual authentication between the card and the PACS biometric terminal, allowing the card to convey back to the PACS cryptographic proof of the biometric verification

In addition, this option may require use of mutual authentication protocols or mutual registration with the PACS.

9.4.4 PIN-to-PACS as Single Factor Knowledge

PACS have used (and in many instances continue to use) a PIN as the primary, single authentication factor as well as a second component in areas where physical access requires two-factor authentication. Several different types of PINs are used, each serving a distinct purpose, and each can be validated in different PACS components. The PIN is entered on a keypad and sent to the PACS for identification, validation, and authorization. In this deployment, the PIN-to-PACS is a unique secret identifier.

This method, which is used by many PACS, does not require a physical token and is not covered by the options in SP 800-116. The method assumes that the identifier (the PIN) assigned to a person is a unique identifier that identifies that person in the PACS authorization database. This unique identifier is also a secret the person has to protect. The person should not use the number for any purpose other than PACS identification; other uses risk disclosing the secret to unrelated entities.

In large organizations, this method may require the person to memorize a large number. PIN length is determined based on the number of users at a site and should be selected to yield an acceptable user-to-permutation ratio.

To further strengthen trust in this method, both the PIV credential and the PACS include a feature that limits the number of invalid PIN entries a system will accept. Should this limit be exceeded, the PIV credential locks. In a PIV credential, this limit is set to three incorrect entries. PACS often allow a user-defined number of attempts before a PIN tamper alarm is generated.

9.4.5 PIN-to-Card

With the PIN-to-card mechanism, a card is presented to the reader and the user provides a PIN for the card to validate. This then unlocks the card and allows the reader to use PIN protected resources from the card (e.g., access to biometric information, execution of an authentication algorithm).

The PIN presentation in itself cannot be considered by the PACS as an authentication method as it is only “user consent” for its card to be used. Unless the card is a trusted entity, the PIN presented to the card has no assurance value for the PACS. The PACS trust in a PIV Card is obtained after a successful card cryptographic authentication requiring a good PIN presentation is executed (using PIV Authentication Key). Because a CAK can be executed without a PIN being presented to the card, only use of the PIV Authentication Key transfers back to the PACS the required trust in the PIN presented to the card.

Trust can be also provided back to the PACS from the card when mutual authentication (trust) is established between a card and the PACS. It is then possible to present a ciphered PIN over the interface

[61] SP 800-73-4 does not allow agency-specific containers to be created in the PIV Card application. In order to have a specific agency container for such purpose, a different card application should be created in the PIV card.

to the card and to receive from the card a cryptographic assurance of the validation of the PIN. Without receiving trusted proof from the card, PIN presentation to the card has no assurance value for a PACS.

9.4.6 Card with PIN-to-PACS

Systems that require secret information (a PIN) in addition to a unique identifier for the user achieve two-factor authentication (what you have and what you know) when the unique identifier is released from a hard-to-clone physical device.

Although details vary from PACS to PACS, the fundamental concept remains the same. The authentication method includes matching both a unique identifier (such as a card number {GUID} or FASC-N) and a PIN. During the process of assigning access privileges to the cardholder, a private PIN is created and included with the unique card number (FASC-N or GUID) and indicates access authorization in the individual's user record. Most PACS store and maintain user records in the PACS control panel. The user access request and PACS process is as follows:

1. A user presents a PIV Card to a PACS reader.
2. The reader processes the card data (signed or unsigned CHUID or CAK, depending on the level of assurance required for the "what you have" factor), and the FASC-N/GUID is released and sent to the PACS control panel[62].
3. The controller uses the FASC-N/GUID to locate and open the user record in the database. The user record includes a private PIN. The system then prompts the user to enter the private PIN.
4. The PIN is sent from the keypad to the PACS control panel for comparison (validation) against the private PIN in the user record.
5. When the PIN entered matches the private PIN, the system initiates the authorization process and makes the access decision.

To further strengthen trust in this method, the PACS includes a feature that limits the number of invalid PIN entries a system will accept. Should this limit be exceeded, the user credential in the PACS locks. PACS often allow a user-defined number of attempts before a PIN tamper alarm is generated.

When the card is also authenticated using a CAK method, this method allows to obtain a two-factor authentication method.

It is worth noting that the PIN is compared only to the single private PIN contained in one individual user record. All other user records remain closed and are untouched by the validation process. The risk of a card being successfully matched with the PIN belonging to a different user is therefore eliminated. To minimize the risk of cardholders forgetting their PINs, some agencies allow people to select their own private PINs.

Like other data, the PIN (or a hash of the PIN) stored in the PACS must be properly protected to avoid inadvertent or unintended exposure. Countermeasures include securing the PIN entry process, supervising both the communication line and the data packet sent from the keypad to controller, and securing the data repositories where user records are stored and maintained.

When a PIN is used in conjunction with a token (as described above), the risk of an exposed PIN is reduced. The PACS will not grant access to a user who enters a PIN without a card or to someone who presents a card without a valid PIN. Both must be entered before the PACS authorization process begins. The process is very similar to that used at an ATM.

This authentication mechanism is described in detail in the "PIV in Enterprise PACS v3"document in its section 10.2.10 (Pattern #11 – CHUID + PIN to PACS) and can be used with a PIV Card in contact as well as contactless mode.

[62] It is also possible to use a CAK authentication mechanism to further strengthen the whole process.

9.5 PACS Provisioning[63]

HSPD-12 and FIPS 201 forced a paradigm shift on PACS. One of the fundamental changes for PACS is the fact identities used for access are not created by the PACS itself when a user is enrolled. The user has a trusted identity represented by his/her PIV Card which has to be registered by the PACS which then attaches to this identity the access rights (access privileges) for this given user. As these identities are maintained (and eventually revoked) by other entities than the PACS, requests received from portal devices when credentials are presented to readers are now subject to more than just a local access privilege verification, but to an end-to-end control procedure that is established locally and connected to the government PIV IT infrastructure.

Traditionally, the PACS for a facility was under the administrative control of a security officer or the director of security for the facility, and typically the credentials issued for use with the PACS were established by the same department or in cooperation with a different department in the same organization. Under these conditions, the processes relating to establishment of an identity for access privileges, the provisioning of the PACS, and managing the life cycle of the credential were isolated to and controlled by the same organization.

This independent process is no longer applicable to a PACS that satisfies FIPS 201 requirements. The main reason is that an identity and the associated identity attributes (i.e., identifiers) are no longer under the control or sole jurisdiction of the PACS owner or administrator. The former closed-loop PACS environment no longer exists. New credentials are created by a process outside of the PACS credentialing and badging environment. As a consequence, the unique identifiers that the PACS relies on to grant access are by default “unknown” to the PACS administrator, and therefore, credentials presented to PACS components are not recognized. To be recognized, they have to be registered (or provisioned) into the PACS by a process that transfers the correct identifiers from the credential into the PACS database so that card or credential profiles within the PACS application can use them to assign and maintain an individual enrollee's access privileges.

Three fundamental methods are used to provision unique identifiers into a PACS application’s database. First, a live, in-person enrollment process can be performed (for HSPD-12, this is the established FIPS 201 process). As part of the enrollment process, unique identifiers are collected or created and transferred through a provisioning mechanism directly to the PACS application database (or transferred to the database from the HSPD-12 identity management system (IDMS) central identity store). This passes the unique identifier created by the FIPS 201 process to the PACS for enabling privilege configuration.

The second method transfers the identity objects or identifiers from a database considered to be the “authoritative database” for the given PACS database. The authoritative database could be a human resources (HR) database that has been provided with the FIPS 201 unique identifiers created by the FIPS 201 process. The HR database now becomes the authority for the PACS database. The identifiers encoded on the card are the same as the identifiers in the PACS database.

The third method transfers identity objects or identifiers from the PIV Card to the PACS database through a provisioning process referred to as “data harvesting” or PIV Card data collection and PACS provisioning. This process identifies the card itself as the authoritative data source, since it was created using a trusted process defined by FIPS 201. To assure that the unique identifiers collected and provisioned into the PACS are usable by the PACS application, middleware is often used between the data harvesting and PACS connection elements to assure that the raw data is parsed and provisioned in accordance with the data model expected by the PACS.

A variety of post-provisioning authentication mechanisms can be enabled, depending on which containers are opened on the PIV Card and what data elements are retrieved and provisioned into the PACS. For example, if all of the digital certificates are captured and stored in the PACS, certificate status can be checked periodically even when the corresponding PIV Card is not present. If an expiration date is

[63] Source: "Authentication Mechanisms for Physical Access Control," Smart Card Alliance Physical Access Council white paper, October 2009

captured and used as the valid date for PACS privilege activation periods, then PACS authorization can be suspended after the expiration date of the PIV Card certificate is reached, in full compliance with FIPS 201 requirements. Stored certificates can also be periodically validated in accordance with the 18-hour window allowed for de-provisioning if a certificate is found to be revoked. For authentication mechanisms to be enabled, authentication objects must first be captured from the credential. Those provisioned in the PACS can be established for automatic and repeated validation, while those captured at the portal and not stored will be checked at the time of access request.

During the provisioning process, manual and automated procedures can be established to assure that the data being captured and provisioned is authentic. If the database-to-database method is used, IT best practices and standards can be implemented to create secure transmission links, and PKI can be used to digitally sign or encrypt the data (e.g., using SSL connections for communications). These procedures follow IT security best-practices models for machine-to-machine communications. If the data harvesting method is used, the expiration date, PIN, facial image, and fingerprint template can be challenged and authenticated when the PIV Card is presented to the PACS.

As part of PKI-based authentication, the certificates available from the credential should also be verified against a valid chain of trust by using path discovery and validation. If the chain can be traced back to a trust anchor, the data source can also be trusted. Performing similar validation checks against the signing certificates also offers assurance that the data has integrity.

The use of established protocol standards, such as online certificate status protocol (OCSP) and server-based certificate validation protocol (SCVP), within the defined infrastructure for cross-certified PKI networks can also enable periodic real-time checks on or downloads of current certificate revocation lists (CRLs). This provides up-to-date status information on issued certificates. To comply with FIPS 201, when any PIV credential certificate is revoked, privileges and authorizations configured in a PACS must be removed within 18 hours of notification of revocation.

9.6 PACS Migration[64]

The transition to FIPS 201 compliant credentials presents unique challenges to security directors with currently-deployed ID badges and existing systems for building access management and control. Key questions that may be asked by all security directors and those responsible for physical access control systems are:

- Will what I have today work with the new directives and requirements? If not, what can I do to comply?
- How do I take advantage of the enhanced security technology in a FIPS 201 credential to improve my organization's security profile?

The answers to these common questions depend on many factors. Compliance methods range from visual presentation and validation of the new PIV Card (a minimal process with high risk), to the trusted process using the PIV Card for fast, electronic authentication through the public key infrastructure (PKI) and a multi-factor reader or handheld device. Beyond reading the PIV card, field devices, the associated network and cabling, intermediary hardware or control equipment, host computers, and processes may be affected by new technologies used by the PIV card.

Given the scope of an enterprise, federated and converged security system, it is thus very important for a security director, facilities manager or systems manager to understand the changes introduced by PIV cards and determine a migration strategy to successfully manage the change. Understanding what will maximize the return on investment and mitigate the risks going forward of “failure of operation” or “failure to comply” is critical to success. It is expected that corollary questions are “how much of my existing

[64] Source: "Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials," Smart Card Alliance Physical Access Council white paper, September 2007, http://www.smartcardalliance.org/pages/publications-pacs-migration-options

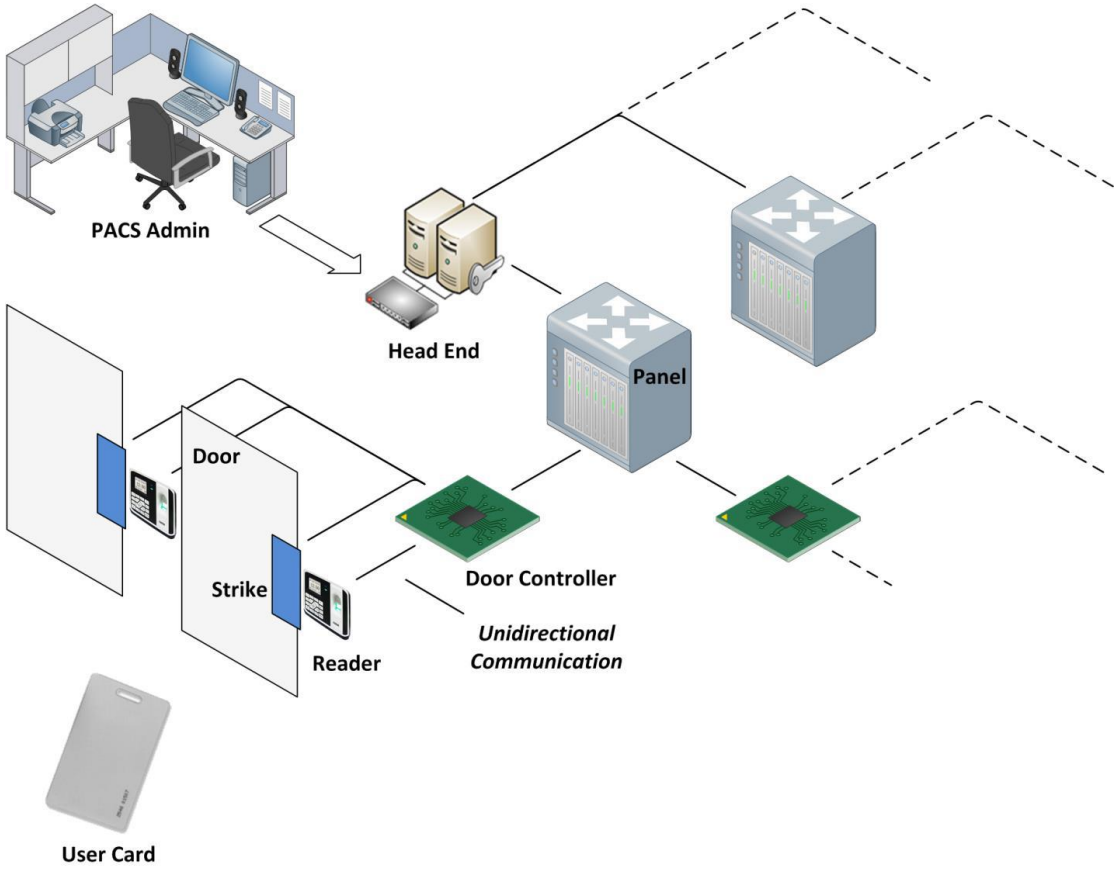
system can I reuse" – i.e., how can I mitigate costs, permitting a migration strategy to be implemented – and optionally "how can I use the same method of authentication for physical access and logical access?"

Simply stated, a migration strategy defines a series of steps in a particular direction leading to a final objective or goal. The final migration goal for Federal agencies is to achieve FIPS 201 compatibility and interoperability by fully using the PIV Card within a PACS. There are a number of migration steps that an agency can take to move toward this goal, while also improving security for the organization. The PIV Card enables agencies to implement a range of identity authentication methods, allowing the method appropriate to an agency's risk assessment and security requirements.

9.6.1 Current PACS Architecture[65]

A typical current PACS architecture will look similar to that shown in the figure below. While different PACS vendors may name their components differently, the essential functionality of all systems is the same.

Figure 7. Typical current PACS architecture



9.6.2 PACS and the Introduction of PIV and PIV-I Cards

The introduction of PIV and PIV-I cards represents major steps forward in standardization of access control within the Federal government. There are now standard identity cards that are recognizable and able to be trusted by all government agencies. While using a PIV or PIV-I card in existing PACS will require changes, it may not necessitate a complete replacement of the PACS components. Figure 8 shows where these changes may affect the system.

[65] The following sections have been extracted from the sections 3.1 to 3.2 of the document "Personal Identity Verification in Enterprise Physical Access Control Systems V3.pdf"

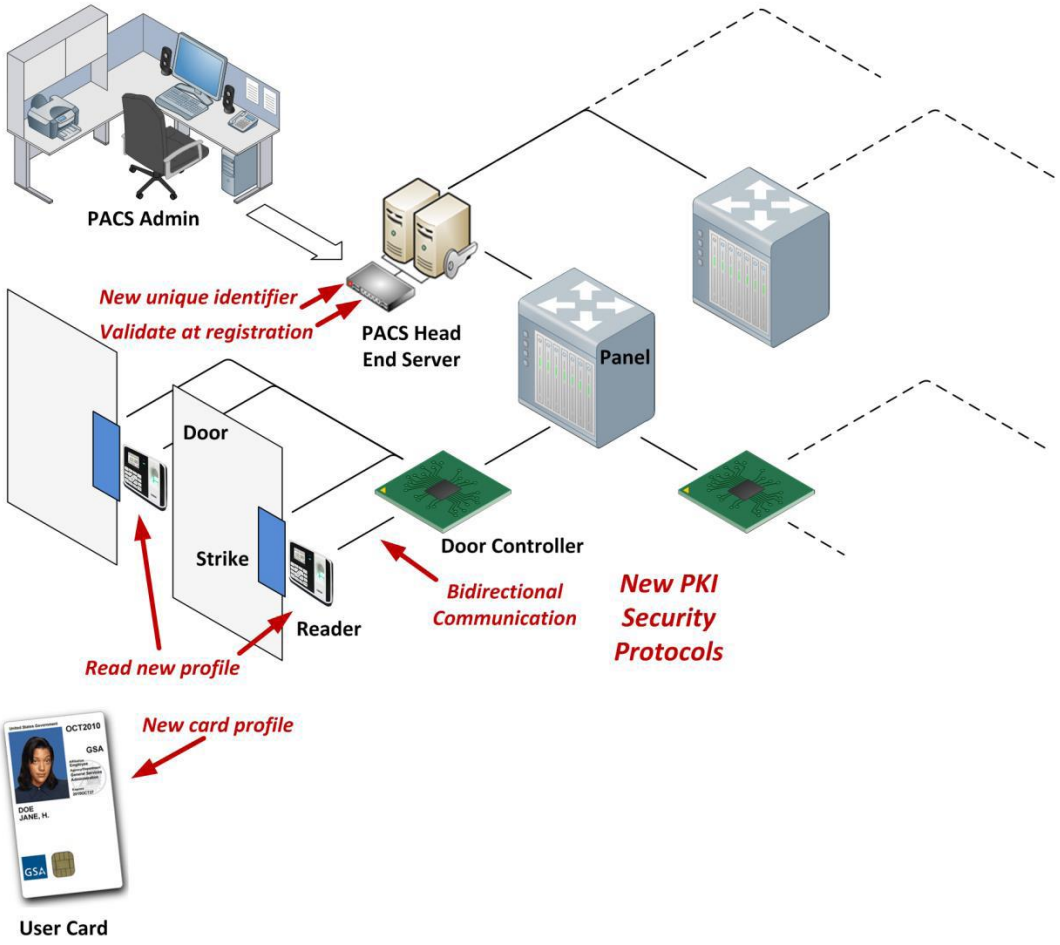


Figure 8. FIPS 201 Changes to PACS

Figure 8 provides only a notional representation of an upgraded PACS. Other architectural models may be followed to reach the target state and the design objectives outlined in the FICAM Roadmap. For example, Figure 8 shows user registration data being entered by the PACS administrator at registration; however, other PACS architectures may allow an agency to use enterprise identity management systems as authoritative identity sources, which push registration data downstream to the PACS head-end server.

Upgrading or replacing an existing PACS to enable it to properly use a PIV or PIV-I card as the user identity card requires a few significant changes:

1. PIV and PIV-I cards are [ISO/IEC 14443] type smart cards with a contactless interface that operates at 13.56 megahertz (MHz). In addition, some authentication mechanisms require using the contact interface. The most common identity cards in use today are contactless proximity cards which operate at 125 kilohertz (kHz). This incompatibility in communication protocol and the need in some cases to support the contact interface will require replacement of the readers.
2. The PIV and PIV-I cards employ a new profile for representing the data on the card. The system must therefore add functionality to read and interpret this new profile.
3. The PACS must be changed to use the Federal Agency Smart Credential - Number (FASC-N) Identifier on the PIV Card as defined in [NIST SP 800-73-3] Part 1 Section 3.1.2.

4. Each PIV-I Card contains a unique identifier called a UUID. The UUID value is in accordance with [RFC 4122] as defined in NIST SP 800-73 section 3.3. This functionality must be added to extract this UUID from the card data, and to use it in the access control decision process.
5. To ensure secure use of PIV and PIV-I cards, some level of authentication and validation must be performed as part of the registration process and in real-time during the access attempt, requiring the ability to extend beyond the immediate physical security boundary in order to retrieve validation objects such as CRLs or Online Certificate Status Protocol (OCSP) responses.
6. The communication protocols between PACS components must be able to process much larger data elements (i.e., the signed Cardholder Unique Identifier [CHUID]).
7. The PACS must support bidirectional communications in order to perform challenge/response activities with PIV and PIV-I cards. This may include updating physical cabling links between the reader and controller/panel and shifting away from the Wiegand Protocol commonly used for unidirectional communication today.
8. The PACS must integrate with the agency's overall ICAM infrastructure, such as enterprise identity management and credentialing systems to provision authoritative identity and credential information and to access shared PKI validation components.

9.6.3 Target PACS Architecture

Figure 9 depicts the target concept for cross-agency access. A PIV Card issued to a user by any agency or a PIV-I Card issued by any trusted issuer can be used for access to various systems at other agencies that have integrated with the Shared Federal Infrastructure – this includes enterprise PACS (E-PACS). Figure 9 is adapted from the technical layer of the FICAM segment architecture ([FICAM Roadmap] Section 3.2.5), which depicts the target concept for cross-agency access.

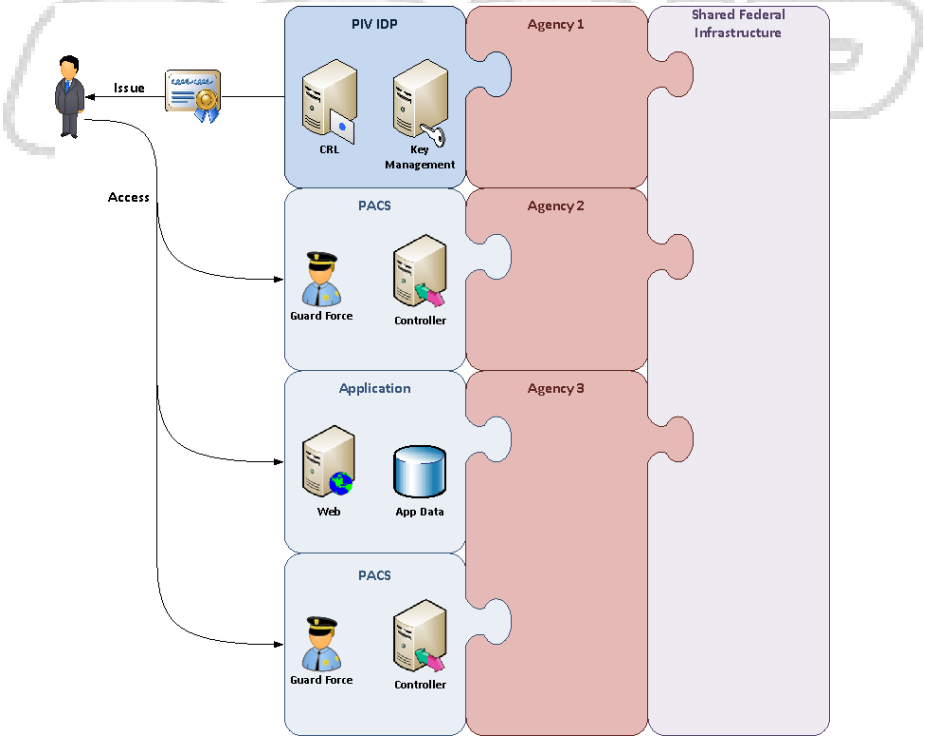


Figure 9. FICAM Roadmap Federal Enterprise Target Conceptual Diagram

The target state for E-PACS includes the following steps:

1. After a determination is made to authorize the cardholder to have access to a facility, the cardholder's credential is provisioned into the PACS. Provisioning may include providing the user with an access account, assigning privileges for access, or access rights to a facility/area.
2. A cardholder desires access to a facility/area and presents his card to the card reader on the attack side (or non-secure side) of the access point.
3. The cardholder presents his/her PIV or PIV-I card (contact or contactless interface) to the card reader. The cardholder is authenticated using one or some combination of authentication mechanisms (see Section 8 for more discussion).
4. Upon successful authentication of the card, the cardholder, and subsequent authorization by the PACS, the controller/panel releases the locking mechanism, the entry point opens, and the cardholder is granted access to the facility/area. If authorization is unsuccessful, the access attempt is denied and the locking mechanism remains locked.
5. The PACS creates a record of the access event based on local audit policy.

10 FIPS 201/PIV Card Use Cases: Logical Access[66]

Agencies have already implemented powerful information technology infrastructures, responding to business challenges that were identified in a number of mandates:

- OMB M04-04, *E-Authentication Guidance for Federal Agencies*, which defines four identity authentication assurance levels for e-government transactions and NIST SP 800-63-2, *Electronic Authentication Guideline*, which provides guidance on the technology to be used for authentication at the different levels of assurance.
- OMB M06-16, Protection of Sensitive Agency Information[67], which calls for encryption of all data on mobile computers/devices that carry agency data and for allowing remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.
- Government Paperwork Elimination Act, which allows digital signatures to be added to online documents and provides the legal framework to accept digital signatures instead of ink signatures.

Security in government IT systems is paramount. Agency network access and information in transit and at rest must be protected. The systems need to ensure that only vetted and authenticated individuals get access to networks, information and facilities. In addition, the agency IT infrastructure supports many processes that streamline transactions, eliminate paper, and improve internal and external business processes.

CSCIP Module 5, "Smart Card Models – Identity and Security," Section 6, includes a detailed discussion of logical access applications and the drivers for using smart card technology for logical access. This section will not repeat the Module 5 content, but will specifically review the PIV Card features that support logical access.

10.1 PIV Card Authentication Mechanisms for Logical Access

HSPD-12 specifically calls for the use of the PIV Card for gaining logical access to Federally controlled information systems. The PIV Card addresses this mandate by providing a hardware token with multiple authentication mechanisms that can support multiple factors of authentication. The PIV Card authentication mechanisms include:

- Cardholder Unique Identifier (CHUID)
- Biometric (fingerprint and iris (optional))
- PKI certificates
  - X.509 Certificate for PIV Authentication
  - X.509 Certificate for Digital Signature (conditional)
  - X.509 Certificate for Key Management (conditional)
  - X.509 Certificate for Card Authentication
  - Secure Messaging Certificate Signer (optional)

[66] Portions of this section are based on content from "Using PIV for Network Access," Anna Fernezian, ActivIdentity, presentation during Using PIV for Physical and Logical Access Workshop at Smart Cards in Government Conference, October, 2008

[67] OMB M06-06, "Protection of Sensitive Agency Information," June 23, 2006, http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf

Table 13 summarizes the authentication mechanisms defined in FIPS 201 and included in the PIV Card to support logical access control. It is implicit that an authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.[68]

Table 13. Authentication for Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism	
	Local Workstation Environment	Remote/Network System Environment
LITTLE or NO confidence	CHUID	-
SOME confidence	PKI-CAK	PKI-CAK
HIGH confidence	BIO	-
VERY HIGH confidence	BIO-A, OCC-Auth, PKI-Auth	PKI-Auth

As defined by OMB M04-04, the PIV Card supports assurance level 4, which requires very high confidence in the asserted identity. The PIV cardholder's identity was rigorously verified by the issuer prior to credential issuance and activation and the PIV Card provides a strong authentication device supporting two or three factor authentication.

10.2 Use of the PIV Card for Logical Access Applications

The PIV Card and its PKI certificates can be used to support multiple logical access applications, including:

- Windows logon
- Password management
- Disk encryption
- VPN authentication
- Email and data encryption
- Electronic signatures for email and documents
- Enterprise single sign-on
- Multi-factor authentication, using one or more authentication factors (card, biometric, PKI certificate, PIN)

While FIPS 201 and NIST special publications to date have not provided implementation guidance on using the PIV Card for logical access, the recently published document, *Federal Identity, Credential and Access Management Roadmap and Guidance*,[69] documents several logical access use cases that are described in the next sections. Addition information on the FICAM guidance document can be found in Section 14.

> *Note: Sections 10.2.1 through 10.2.4 were extracted from Federal CIO Council document, "Federal Identity, Credential and Access Management Roadmap and Guidance."*

10.2.1 PKI Credentials

PKI certificates can be issued as software, or "soft" certificates, where the private key of the PKI key pair is installed as part of a software application, usually directly to a computer or other devices, or as hardware certificates, where the private key is installed on a protected hardware token (e.g., a PIV card)

[68] Source: FIPS 201, page 51

[69] "Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance," Version 2.0, Identity, Credential and Access Management Subcommittee (ICAMSC), Federal CIO Council, December 2, 2011, http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf

that has been tested and certified to be FIPS 140 compliant. Current Federal PKI users may or may not use the PIV Card certificates for logical access applications.

According to the FICAM guidance document, in the future, it is intended that agencies will eliminate the issuance of separate PKI credentials to internal users and that scenarios that require the use of PKI credentials will be addressed using the PKI certificates commonly found on the PIV card:

- PIV Authentication Key (mandatory) – Used for PACS and smart card logon in LACS.
- Card Authentication Key (mandatory) – Used for PACS applications.
- Digital Signature Key (mandatory/conditional[70]) – Used for digital signatures.
- Key Management Key (mandatory/conditional) - Used for managing the keys on the card. This key is often also used for encryption in email and documents.
- Secure Messaging Key (optional) - Used to establish a secure session (confidentiality and integrity) between the card and the client application. Also provides card authentication as the card key pair used by the card has a certificate verifiable by the client application.

10.2.2 Password Tokens for Logon

The term "password token" is derived from SP 800-63. A password token is a secret that a claimant memorizes and uses to authenticate his or her identity, and thus falls into the credential category of "something you know," whereas the PIV and PKI credentials are considered credentials in the category of "something you have." Common password tokens are username/password combinations. Password tokens are typically created specifically by and for the application being accessed and the process is often closely tied to creation of a digital identity record and user account within the application.

Currently, application owners primarily control the creation and issuance of password tokens to users, which leads to stove-piped credentialing processes. Some application passwords are managed via major applications across an enterprise for internal users (e.g., Windows logon), and in some limited current scenarios there are external (business, citizen) initiatives that provide password tokens centrally and allow their use by multiple applications; however, the norm is for each application to manage its own access and password management processes. Today, most federal applications for both internal and external user groups are accessed using passwords, and as a result, password management is a primary activity for application owners/administrators. In addition, many username and password issuance processes do not incorporate required identity proofing, are not mapped to federal authentication assurance levels and can be easily compromised.

Password maintenance processes are also usually different for each application in the enterprise, resulting in redundant infrastructures and high maintenance costs.

According to the FICAM guidance document, in the future, the use of passwords for internal users will be minimized in favor of other identity credentialing solutions. For internal efficiencies and effectiveness (the Federal employee community as constituent/user), application owners and administrators will migrate away from password based access control systems to an identity and access management solution that utilizes the capabilities of the Federal PIV card.

10.2.3 Logical Access to Networks, Systems, Applications and Data

Government agencies currently use a variety of mechanisms for granting logical access, many of which are tied to a specific application. Typically, an application is set up to use only one type of credential. As was discussed in Section 10.2.2, a user ID/password combination is most prevalent. Other types of tokens currently in use at agencies for granting logical access include:

- A one-time password generator

[70] The Digital Signature Key as well as the Key Management Key are both mandatory if the cardholder has a government issued e-mail address.

- An approved and internally-issued PKI soft certificate
- Biometric matching
- A trusted smart card
- USB tokens and other hardware tokens holding PKI certificates
- A trusted externally issued PKI soft certificate
- A trusted third party credential (independently provided identity assertion)

Access to both support- and mission-focused systems is typically granted at the application level. As a result, logical access systems in the current state are in many cases synonymous with the built-in individual application access mechanisms. Some notable exceptions, such as Windows logon, are in most cases centrally managed and provisioned. Once a user has been granted access to the network, however, individual applications both within and outside the agency require additional identity authentication frequently using additional unique user IDs and usually requiring additional unique passwords. This model requires users to possess or remember numerous credentials in order to carry out daily functions.

According to the FICAM guidance document, in the future, granting logical access includes two main models. For internal users, it is intended that agencies will leverage the various capabilities of the PIV card, particularly the PIV authentication digital credential, to grant access to applications at all levels of assurance. A key goal is enabling single sign-on for federal users of applications.

For external users, it is intended that agencies will adopt a model for federated identity, accepting third party credentials from external parties. A key goal for external users is to be able to access a variety of government services using a reduced set of login credentials and to reuse existing credentials issued by a third party provider. Over time, it is anticipated that certain external users within the government-to-government (G2G) and government-to-business (G2B) sectors will possess PIV-interoperable credentials. Wherever possible, these credentials should be leveraged to maximize interoperability. Work is ongoing to develop acceptance criteria for third party credential types that are suitable for use by other external users at each of the four identity assurance levels outlined for federal systems within OMB M-04-04 and NIST SP800-63.

The target process flow for using the PIV Card for logical access is as follows:

1. A user attempts to access an agency network or application. The logical access control system (LACS) prompts the user to provide a valid credential to perform user authentication.
2. The user inserts the PIV Card into a card reader. In order to allow access to certain authentication mechanisms available on the contact chip, the user inputs the PIN.
3. The LACS validates the PIV Card using one or a combination of the following authentication mechanisms available on the card and the appropriate authentication techniques:
    a. PIV Authentication Key
    b. Card Authentication Key
    c. Biometric check

    A separate authentication may be bypassed in instances where a current session has been established based upon previous authentication events.
4. The LACS determines the business rules needed to approve access to the application, including scheme translation, required attributes, and access control policies. Once the User has been successfully authenticated, the LACS sends an assertion that includes any required attributes to the application that the user is trying to access.

5. The application verifies the user's permissions and approves or denies the access attempt based on business rules and internal directories.
6. The LACS records the access event.

10.2.4 Secure Document or Communication with PKI

Encryption is the process of transforming data from a readable form into a protected form that requires an individual to possess the correct cryptographic key in allowing to read it. It is used to provide confidentiality for data. A digital signature is the result of a cryptographic mechanism adding to an information some data (signed data hash value of the information) in order to provide origin authentication of origin, information integrity, and signatory non-repudiation. The PIV Card described in the previous sections of this document is the PKI credential its owner can use as the tool providing for digital signatures and encryption.

The target process flow for using the PIV Card for signing a file or communication is as follows:

1. The user opens the application that will be used to digitally sign the data (e.g., Outlook).
2. The user inserts the PIV Card into card reader, and selects the appropriate alternate private key to be used for signing. If the certificate has been pre-registered, the application may automatically select the appropriate certificate.
3. The user selects the option to digitally sign the data.
4. The application hashes the data and uses the user's private key to encrypt the resulting message digest, thus creating the digital signature.
5. The user transmits the original data (which may or may not be encrypted) along with the digital signature to the intended recipient.
6. The recipient opens the file and verifies signature. The recipient first duplicates the creation of the message digest. Then the recipient decrypts the digital signature using the user's public key and compares it to the duplicated message digest. If the two match, the document has not been altered and was signed using the user's private key.

10.2.5 Other Uses of the PIV Card for Logical Access Applications[71]

The PIV card's PKI certificates, biometrics, PIN and secure data storage can enable many logical access applications.

10.2.5.1 Remote Access from Computers on Untrusted Networks

The PIV Card can be used to provide secure virtual private network (VPN) access, either using PKI authentication.

10.2.5.2 Disk Encryption

Agencies face a liability exposure from lost or stolen computers that contain sensitive data. The PIV Card encryption certificate can be used to protect the key used for disk encryption, providing multi-factor authentication and leveraging the agency's PIV infrastructure for security and key management.

10.2.5.3 Single Sign-on

Government employees need to access information on many disparate systems, typically with multiple user passwords since many applications are not PKI-enabled. Currently enterprise single sign-on (E-

[71] Source: "Using PIV for Network Access," Anna Fernezian, ActivIdentity, presentation during Using PIV for Physical and Logical Access Workshop at Smart Cards in Government Conference, October, 2008

SSO) solutions are used to make multiple system access more convenient to users. PIV cards can be used with E-SSO solutions, with the E-SSO middleware leveraging the PIV Card for network authentication and using the PIV Card for automated and secure presentation of passwords to applications.

10.2.5.4 Printer Authentication

The Department of Defense recognized key security weaknesses with printers: a very secure document could be printed and retrieved by an unauthorized user or a multi-function printer could be used to scan and then email a secure document. Intelligent printers are available that are implementing PIV and Common Access Card middleware so that the PIV Card and CAC can be used to authenticate users before they can collect print-outs.

11 FIPS 201/PIV Card and Services Certification, Testing and Product Acquisition

Both NIST and GSA have established evaluation programs for the testing and evaluation of specific products and services needed to implement HSPD-12 and FIPS 201.

11.1 NIST Personal Identity Verification Program (NPIVP)[72]

NIST has established the NIST Personal Identity Verification Program (NPIVP) to test and validate PIV components and sub-systems required by FIPS 201.

The objectives of the NPIVP program are:

- To validate the compliance/conformance of two PIV components – PIV middleware and PIV Card application – with the specifications in NIST SP 800-73
- To provide assurance that the set of PIV middleware and PIV Card applications that have been validated by NPIVP are interoperable.

All of the tests under NPIVP are handled by third-party test facilities that are accredited under the Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP) established by the National Voluntary Laboratory Accreditation Program (NVLAP)[73] and have extended their scope of accreditation to include the PIV test methods.

NIST has published derived test requirements as NIST SP 800-85 A-1: PIV Card Application and Middleware Test Guidelines and SP 800-85 B: PIV Data Model Test Guidelines.

The status and results of these tests and product validation are posted at the NIST NPVIP website: http://csrc.nist.gov/npivp/.

11.2 FIPS 140-2[74]

FIPS 140-2 is the U.S. government security certification standard for assuring the correct implementation of any cryptographic module. It applies to all of the cryptographic operations of the smart card integrated circuit and related operating system and application software, such as applets on a Java Card. FIPS 140-2 also applies to any other cryptographic module used in a FIPS 201 system, such as a dedicated hardware security module (HSM). Under Federal Information Security Management Act (FISMA) rules, any product used in the Federal government employing cryptographic functions must obtain a FIPS 140-2 certification. In the late 1990s, smart card manufacturers began submitting smart cards for FIPS 140-1 certification. In 2001, FIPS 140-1 was updated to FIPS 140-2.

FIPS 140-2 specifies the requirements for cryptographic modules in the areas of secure design and implementation, including module specification; ports and interfaces; roles, services, and authentication; finite state model; physical security; operational environment; cryptographic key management; electromagnetic interference/electromagnetic compatibility (EMI/EMC); self-tests; design assurance; and mitigation of other attacks.

FIPS 140-2 specifies four levels of security. The standard does not specify what level is required by any particular application.

- Level 1 imposes very limited requirements; all components must be “production-grade” and obvious security functions must be present. Level 1 restricts the machine on which the module runs to operating in single-user mode.

[72] Source: NIST web site, http://csrc.nist.gov/groups/SNS/piv/npivp/index.html
[73] http://www.nist.gov/nvlap/index.cfm
[74] Sources: "What Makes a Smart Card Secure?," Smart Card Alliance white paper, October 2008; FIPS 201, p. 64

- Level 2 adds requirements for physical tamper-evidence and role-based authentication. It is noticeably harder to obtain. The difficulty is not necessarily with the cryptographic module code, but rather with the formalities required and the fact that Level 2 modules must run on validated hardware under validated operating systems.
- Level 3 adds requirements for physical tamper-resistance and identity-based authentication. Level 3 also requires physical or logical separation between the interfaces by which certain security parameters enter and leave the module.
- Level 4 imposes much more onerous physical security requirements and requires more robust security features to defend against various environmental attacks.

Cryptographic modules receive security level ratings that reflect the requirements they meet. Most smart cards (secure IC plus operating system plus application software) that are certified by FIPS 140-2 are certified to either Level 2 or Level 3.

FIPS 201 specifies that all of the cryptographic modules in the PIV system (both on-card and issuer software) be validated to FIPS 140-2 with an overall security level 2 (or higher). The facilities for FIPS 140-2 testing are the Cryptographic Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) program of NIST. Vendors wanting to supply cryptographic modules for the PIV system can select any of the accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor module is issued by the Cryptographic Module Validation Program (CMVP),[75] a joint program run by NIST and Communications Security Establishment (CSE) of the Government of Canada. The details of the CMVP and NVLAP programs and the list of CMT laboratories can be found at the CMVP Web site at http://csrc.nist.gov/groups/STM/cmvp/index.html.

11.3 FIPS 201 Evaluation Program[76]

The Office of Management and Budget (OMB) has designated the General Services Administration (GSA) as the Executive Agent for government-wide acquisitions for the implementation of HSPD-12. Additionally, OMB has directed Federal agencies to purchase only products and services that are compliant with the Federal policy, standards and supporting technical specifications.

NOTE: The GSA FIPS 201 program is currently undergoing a major shift in that component testing for the purpose of posting to an Approved Product List (APL) is being discontinued and replaced by an end-to-end system solution approval process. This shift was determined necessary as relying parties were not happy with the “menu” approach for picking components, especially when a solution was put together by a department or agency using GSA APL components that later was determined not to work for reasons of cross compatibility.

The FIPS 201 Evaluation Program is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within GSA. The goal of the FIPS 201 Evaluation Program is to evaluate products and services against the requirements outlined in FIPS 201-1 and supporting documents. In addition to derived test requirements developed to test conformance to the NIST Standard, GSA has also established interoperability and performance metrics to further determine product suitability.

Once evaluated and approved by the FIPS 201 Evaluation Program, products and services are placed on the FIPS 201 Approved Products List (APL). Agencies can then procure these products and services from suppliers for their HSPD-12 implementations having full assurance that they meet all of the requirements of FIPS 201-1 as well as the GSA interoperability and performance criteria.

GSA has designated third-party laboratories for the evaluation and testing of products and services under

[75] http://csrc.nist.gov/groups/STM/cmvp/index.html

[76] Sources: "FIPS 201 Evaluation Program - Supplier Policies and Procedures Handbook," Version 5.0.0, December 12, 2008, http://fips201ep.cio.gov/documents/Suppliers_Handbook_v5.0.0.pdf; GSA FIPS 201 Evaluation Program web site, http://fips201ep.cio.gov/; OMB M06-18, "Acquisition of Products and Services for Implementation of HSPD-12," June 30, 2006, http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-18.pdf

the FIPS 201 Evaluation Program. Vendors must submit completed application packages and, as appropriate, products if laboratory testing is required.

The previous component based testing and approval process is detailed here for historical reasons.

Based on the requirements extracted from FIPS 201-1 and its supporting special publications, the GSA FIPS 201 Evaluation Program was performing evaluations in 24 different product and service categories. Specific evaluation and approval requirements for each of the categories of products/services were established and publicly posted by GSA. Each approval procedure cites the specific FIPS 201 requirements that are evaluated for that category of product/service and the type of evaluation needed for approval.

The categories of products/services for the FIPS 201 Evaluation Program and approval procedures for all of those categories were posted at the FIPS 201 Evaluation Program website: http://fips201ep.cio.gov/ now replaced by the new approval procedures: http://www.idmanagement.gov/ficam-testing-program.

11.4 GSA Approved Product List[77]

GSA has established the FIPS 201 Approved Products List (APL) for all products and services that have been approved under the GSA FIPS 201 Evaluation Program. The purpose of the GSA APL for FIPS 201 products and services is to ensure agencies can obtain interoperable products and services from a number of suppliers with full confidence of correct and uniform implementation. GSA will continue to evaluate and approve products/services as completed submissions are received; all approved products are posted to the APL. The APL can be accessed at: http://www.idmanagement.gov/approved-products-list.

There are other types of services that may be necessary for HSPD-12 systems and deployments, but have no normative requirements specified in FIPS 201 and, therefore, are not included in the FIPS 201 Evaluation Program (e.g., integration services, contractor managed services and solutions). Qualification requirements for these services and a list of qualified vendor services are also posted at: http://idmanagement.gov.

11.5 PIV Card Infrastructure and Issuance

Federal agencies need to put in place an infrastructure to credential employees to the FIPS 201 standards. Agencies have taken two approaches: developing their own infrastructure or using the GSA USAccess managed service. As of March 2010, OMB reports that 24 agencies are using independent infrastructure (including DoD, Department of State, DHS, Department of Health and Human Services, NASA and the Social Security Administration) and 64 agencies are using the GSA service (including the Department of Commerce, Department of Energy, Department of Justice, Interior and Treasury).[78] Any FIPS 201 infrastructure involved with PIV Card issuance must obtain FIPS 201 certification for one or both of the following services: (1) graphical personalization, (2) electrical personalization.

The GSA USAccess service[79] is a complete end-to-end service to issue fully compliant identity credentials for government employees and contractors. By participating in the USAccess program, agencies may benefit from a centralized program and economies of scale for credential management. Furthermore, USAccess provides a key foundational component to help agencies unite its logical and physical access control system implementation strategies. GSA USAccess services include:

[77] Sources: GSA FIPS 201 Evaluation Program web site, http://fips201ep.cio.gov/; OMB M06-18, "Acquisition of Products and Services for Implementation of HSPD-12," June 30, 2006, http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-18.pdf

[78] "HSPD-12 Implementation Status Reports," OMB, http://www.whitehouse.gov/omb/e-gov/hspd12_reports/

[79] GSA USAccess web site, http://www.fedidcard.gov/

- System infrastructure: Provides a secure, standards-based enterprise identity management capability with various PIV-related components implemented with high availability and disaster recovery capabilities.
- Credential production, issuance, activation and management
  - Automatically batches and processes PIV credential requests, produces the credential in a central facility, and ships to designated agency locations.
  - Once the applicant receives the credential, his/her identity is confirmed using biometric verification followed by credential "personalization" with the applicant's biographic information, fingerprint templates, and PIN and generation of the suite of digital certificates.
  - Credential management activities, such as suspensions, reprints or revocations, may be performed by authorized role holders via an intuitive user interface.

12 PIV-I: Interoperability beyond the Federal Government

Organizations outside of the Federal government can benefit from following the FIPS 201 standard and issuing interoperable identity credentials. Following the FIPS 201 process for credential issuance allows all Federal relying parties to trust the credential, across organizations. This trust is established by an enrollment, registration, and issuance process that is trusted across organizations, and a strong authentication credential that leverages a cross-certified and federated public key infrastructure. A PIV interoperable (PIV-I) credential can be of great value to organizations that collaborate or do business with the Federal government and have a requirement to issue interoperable identity credentials.

NOTE: PIV-I is not a standard but a special configuration of PIV defined by the CIO council in a guideline document described below.

FIPS 201 provides a defined framework and technical specifications for organizations to follow to issue and use interoperable credentials. By basing identity credentialing efforts on FIPS 201, organizations can:

- Follow a proven process for identity vetting
- Implement an identity vetting process that provides the basis for trusting identities across organizations or with Federal agencies
- Implement an identity credentialing solution that is interoperable with and compatible across organizations or with Federal agencies
- Acquire proven products and services that meet FIPS 201 technical specifications from multiple vendors

The First Responder Authentication Credential (FRAC) is one usage scenario of a PIV-I credential which is successfully driving adoption in the state, local and commercial sectors. Early adopter organizations issuing FRAC/PIV-I cards to date have attempted to closely align with the maturing PIV-I recommendations to ensure current and future interoperability and trust. As discussed further in Section 15.3, PIV-I credentials are enabling emergency responders from early adopter Federal agencies, state and local governments, and commercial organizations (e.g., health and medical services providers, banking and financial services providers) to verify their identities at demonstration incident sites.

As a result of non-federal issuers (NFIs) of identity cards expressing a desire to produce identity cards that can technically interoperate with Federal government PIV systems and may be trusted by Federal government relying parties, the Federal CIO Council published the guidance document, *Personal Identity Verification Interoperability for Non-Federal Issuers,* in May 2009.

> *Note: The following sections (12.1 and 12.2) are redacted version of extracts from the document, Personal Identity Verification Interoperability for Non-Federal Issuers, published by the Federal CIO Council in July 2010.*[80]

12.1 PIV Interoperability for Non-Federal Issuers (NFI)

As the Personal Identity Verification (PIV) initiative progresses, it is garnering a great deal of interest from parties external to the Federal government. These non-federal organizations want to issue identity cards that are (a) technically interoperable with Federal government PIV systems, and (b) issued in a manner that allows Federal government relying parties to trust the cards. Furthermore, such interoperability and trust may be driven by operational imperatives of great interest to the Federal government (e.g. First Responder Authentication Card (FRAC)). However, the PIV Card standard, Federal Information Processing Standards (FIPS) 201, is limited in scope to the Federal government and has several requirements that can be addressed only by the Federal government community. Therefore, some

[80] "Personal Identity Verification Interoperability for Non-Federal Issuers," CIO Council, Version 1.1 July 2010, http://www.idmanagement.gov/sites/default/files/documents/PIV_IO_NonFed_Issuers.pdf

guidance is needed to assist non-federal issuers of identity cards in achieving interoperability with Federal government PIV systems.

The guidance document provides solutions for overcoming the barriers to federal reliance on non-federal identity cards in four specific areas:

1. **Common terminology for identity cards.** In order to ensure consistency, a lexicon for differentiating a Federal government PIV Card from a non-federally issued identity card seeking PIV system interoperability must be developed;
2. **Technical requirements**. For non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met;
3. **Identifier namespace**. Effective use of identity cards requires an identifier that is unique across all identity cards. Lack of a unique identifier may result in incorrect access control decisions; and
4. **Trusted identity**. The fundamental purpose of an identity card is to establish the identity of the cardholder. Therefore, an identity card must be issued in a manner that provides Federal government relying parties with a requisite level of trust.

For each of these, a minimum set of requirements has been described that will allow NFI identity cards to technically interoperate with Federal government PIV systems and be trusted by Federal government relying parties.

12.2 Minimum NFI Card Requirements

Federal government reliance (trust) on NFI identity cards requires the card to technically comply with PIV specifications so as to technically interoperate with Federal government PIV systems, and to have specific trust elements. The Federal Bridge Certification Authority (FBCA) certifies NFIs for use by Federal relying parties. The FBCA Certificate Policy (CP) contains the detailed requirements that those NFIs must meet.

The following sub-sections summarize those requirements.

12.2.1 Common Terminology for Identity Cards

In order to ensure consistency, a lexicon for differentiating a Federal government PIV Card from a non-federally issued identity card seeking PIV system interoperability must be developed. A major issue in the identity card space is the lack of standard terminology to unambiguously distinguish between characteristics (e.g., trust characteristics) of federally issued and NFI identity cards. The result can be confusion, uncertainty, or misunderstanding regarding the capabilities and trustworthiness an identity card encompasses – particularly an NFI identity card. Attaining clarification after the fact can be costly in many ways (e.g., investing and implementing with an incorrect understanding likely requires rework or abandonment). PIV standards clearly define the federally issued PIV Card. However, the definition of different NFI identity cards, especially regarding their relationship to PIV remains problematic. This document resolves the terminology problem by proposing a more complete set of identity card terms that unambiguously describes federal and NFI identity cards in terms of critical characteristics affecting the degree of federal relying party trust. The proposed terms are:

- **PIV Card** – an identity card that is fully conformant with federal PIV standards (i.e., FIPS 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure that PIV cards are interoperable with and trusted by all Federal government relying parties.
- **PIV interoperable (PIV-I) card** – an identity card that meets the PIV technical specifications to work with PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government relying parties to trust the card.

- PIV compatible card (now named **CIV for Commercial Identity Verification card)** [81]– an identity card that meets the PIV technical specifications so that PIV infrastructure elements such as card readers are capable of working with the card, but the card itself has not been issued in a manner that assures it is trustworthy by Federal government relying parties.

A PIV interoperable card builds upon a CIV card. An NFI must procure a CIV card and issue it in a trustworthy manner. NFI CIV cards and NFI PIV interoperable cards are not "PIV cards" because NFIs and their identity cards cannot directly meet certain Federal government PIV requirements.

An NFI CIV card is not a PIV interoperable card. An NFI PIV interoperable card can be trusted by Federal government relying parties because it has the minimum set of PIV trust elements. An NFI CIV card cannot be trusted by Federal government relying parties because it lacks the minimum set of PIV trust elements[82].

12.2.2 Assumptions

The following assumptions apply:

1. Each Federal government relying party determines the extent to which it will trust PIV interoperable cards within its areas of control;
2. Cardholder privileges in any particular situation are determined solely by the Federal government relying party (i.e., PIV interoperable cards do not guarantee access of any kind, nor do they prevent issuance of a PIV card); and
3. Each Federal government relying party makes access decisions based on the ability to verify the validity of the PIV interoperable card and on local access policy for external organizations.

12.2.3 Requirements for NFI Cards

The following requirements apply to NFIs:

1. NFI PIV compatible cards and NFI PIV interoperable cards will use a smart card platform that is technically compatible with NIST technical requirements outlined in Section 12.2.4;
2. Consistent with the policy directives in Office of Management and Budget (OMB) memorandum M-05-24, NFI PIV interoperable cards should contain distinctive markings indicating the identity of the issuing entity; and
3. NFI PIV interoperable cards are electronically personalized, as defined by FBCA Appendix A and supporting documents.
    a. NFI PIV interoperable cards will include an authentication digital public key infrastructure (PKI) certificate that meets a minimum set of criteria identified in Section 12.2.6.
    b. NFI PIV interoperable cards will include biometric fingerprint information that conforms to NIST Special Publication SP 800-76.

12.2.4 Technical Requirements for NFI Cards

For non-federally issued identity cards to interact with federal infrastructure, basic technological requirements must be met. NFI identity cards must conform to the NIST technical specifications for a PIV Card as defined in NIST SP 800-73 and meet the cryptographic requirements of FIPS 140 and NIST SP

[81] The term CIV (Commercial Identity Verification) is now used to replace the previous name given to these cards: PIV-C for PIV-Compatible. See document from the Smart Card Alliance: http://www.smartcardalliance.org/resources/pdf/CIV_WP_101611.pdf

[82] The issuance process and identity proofing are not controlled for CIV cards. The PIV-I Card has the same issuance and identity process as PIV Cards, but may not have the same background checks used for a PIV Card.

800-78. In order to ensure this conformance, NFIs should refer to the General Services Administration (GSA) Approved Products List (APL) available at www.idmanagement.gov.

12.2.4.1 Required Electronic Features

NFI PIV interoperable cards must be populated in accordance with NIST SP 800-73 and contain, at a minimum, the following:

- Biometric;
- Card Holder Unique Identifier (CHUID);
- Universally Unique Identifier (UUID);
- Authentication PKI Certificate[83] mapped to the PIV-I Hardware Policy[84];
- Card Authentication Certificate mapped to the PIV-I Card Authentication policy;
- Facial Image Buffer;
- Security Object; and
- Card Capability Container.

12.2.4.2 Required Physical Features

The physical topography of NFI PIV interoperable cards must include, at a minimum, the following:

- Organization Affiliation (if exists; otherwise the issuer of the card)
- Card holder facial image
- Card holder full name; and
- Card expiration date.

NFI PIV interoperable and CIV card visual distinction is required to ensure no suggestion of attempting to create a fraudulent PIV card.

12.2.5 Identifier Namespace

Effective use of identity cards requires an identifier that is unique across all identity cards. Lack of a unique identifier may result in incorrect access control decisions. The PIV Card includes a Federal Agency Smart Credential - Number (FASC-N) to uniquely identify it, and thus avoid identifier namespace collisions. When managed and distributed within a closed system (the U.S. government), uniqueness is ensured. However, the FASC-N structure does not support its use beyond the U.S. government as it cannot be easily extended to allow sufficient identifier namespace to support a large NFI population. In addition, NFIs cannot consistently assign globally unique FASC-Ns. Consequently, there is a need to develop a smart card numbering scheme comparable to the FASC-N that follows a set of guidelines that ensure uniqueness across the federal issuers and NFIs.

12.2.5.1 Use of the UUID by NFIs

NFIs shall include a valid RFC 4122 generated UUID in accordance with NIST SP 800-73 section 3.3 in the GUID field of the CHUID. In addition, NFIs must include the UUID in a subject-alt-name extension of the authentication certificate in accordance with PIV-I Profile to ensure UUID availability to relying parties in remote Logical Access Control System (LACS) environments.

[83] The Authentication PKI Certificate functionally is similar to the PIV Authentication Certificate, requiring cardholder authentication (e.g., PIN) to the cryptographic module before activation of the private key.
[84] NFI certificate policies are defined in FBCA CP.

12.2.5.2 Use of the FASC-N Field by NFIs

NFIs must generate and use a FASC-N conformant with NIST SP 800-73. If a Federal government relying party PACS is capable of processing NFI PIV interoperable cards, only the UUID may be relied upon as a unique card identifier. Otherwise, the Federal government relying party should consider alternative risk-based solutions.

The following text from "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems v2.2," referenced by NIST SP 800-73, establishes FASC-N construction rules for NFIs:

> "The FASC-N is not designed to insure uniqueness for non-federal issuers. For non-federal issuers, additional tag length value (TLV) elements must be specified to insure uniqueness of the FASC-N. If an Agency Code of 9999 is present in the FASC-N, then the DUNS TLV record in the CHUID container will indicate the identity of the card issuer. It is anticipated that the Tag 30 TLV record will always exist for industry compatibility for PACS that use the System Code and Card Number as a card identifier.
>
> For issuers not defined in SP 800-87, a FASC-N can be constructed using an Agency Code of 9999; however, this will not provide uniqueness of the FASC-N for federal agency applications. If a non-federal issuer has a requirement for federal interoperability, then a sponsoring agency may assign a specific System Code(s) to the issuer. When an Agency Code of 9999 is specified, an issuer must include an additional TLV record in the CHUID[85], such as the DUNS, to insure uniqueness of the CHUID. It is the responsibility of the sponsoring agency to maintain records of specific System Code assignments for both internal and external issuers of FASC-Ns".

The above rules create a serious identifier namespace collision risk about which relying parties should be aware. For access control purposes, legacy PACS often only read 14 digits consisting of the agency code, system code, and credential number. The FASC-N rules for NFIs do not ensure uniqueness for those 14 digits across issuers, creating the potential for two different people having the same identifier for legacy PACS when the FACS-N is used as the card identifier. Federal government relying parties are encouraged to consider this issue and make local risk-based decisions regarding NFI PIV interoperable cards and their legacy PACS when they do not use the card UUID as the card identifier.

If a Federal government relying party PACS is capable of processing NFI interoperable cards, the GUID should be relied upon as a unique card identifier. Otherwise, the Federal government relying party should consider alternative risk-based solutions.

12.2.6 Trusted Identity

The fundamental purpose of an identity card is to establish the identity of the cardholder. Therefore, an identity card must be issued in a manner that provides Federal government relying parties with a requisite level of trust. To trust any identity card, it must be possible to validate the card (i.e., not expired, not revoked) and authenticate the cardholder (i.e., the cardholder is who he or she says he or she is). The PIV Authentication Certificate is where "trust" in the PIV Card resides. However, the policy object identifier (OID) for the PIV Authentication Certificate is available only to Federal government organizations. Therefore, a comparable identity PKI authentication certificate that can be trusted by Federal government relying parties is identified and used by NFIs.

In addition, trust in an identity card requires an understanding and acceptance of the process used to determine the accuracy of the claimed identity. For the Federal government PIV card, FIPS 201 specifies identity proofing and background vetting processes. While NFIs are unable to mirror the background vetting process (e.g., the National Agency Check with Written Inquiries (NACI)) employed by the Federal government, they can and must perform identity proofing in a manner that promotes trust in the process.

[85] The uniqueness issue of the CHUID for NFIs is solved by using the GUID (with a populated UUID) as the unique credential identifier, and does not require any additional information from the FASC-N

Accordingly, NFIs require a common identity proofing standard that is understood by and acceptable to the Federal government.

12.2.6.1 NFI Identity Authentication PKI Certificate

NFI PIV interoperable cards must include an identity authentication PKI certificate issued by a certification authority (CA) that chains to the Federal Bridge Certification Authority (FBCA) at the PIV-I Hardware policy via cross-certification. This will enable Federal government relying parties to verify the validity of the identity card via the identity authentication PKI certificate by first verifying the issuing organization (i.e., CA cross-certified with FBCA), and then providing assurance that the certificate (and by extension, the card) has not been revoked or invalidated since issuance.

The identity authentication PKI certificate in an NFI PIV interoperable card contains a policy object identifier (OID) other than the one mandated for Federal PIV authentication use, which contributes to satisfying the electronic distinctiveness requirement for the NFI PIV interoperable card.

12.2.6.2 Ensuring Identity Validity

The Federal government's identity proofing and background vetting processes, as defined in FIPS 201, are two distinct activities.

12.2.6.2.1 Identity Proofing

During identity proofing, the applicant is required to appear in person and provide two forms of identity source documents in original form from the list of acceptable documents defined in FIPS 201-2[86]. At least one of the documents must be a valid state or Federal government-issued picture ID. This identity proofing process is commensurate with OMB Memorandum M-04-04, E-Authentication Guidance for Federal Agencies, Assurance Level 4, which in turn provides the common identity proofing standard for NFIs.

NIST SP 800-63 defines E-Authentication Assurance Level 4 identity proofing as:

- In-person appearance and verification of:
  a) A current primary government picture ID that contains applicant's picture, and either address of record or nationality of record (e.g., driver's license or passport), and;
  b) Either a second, independent government ID document that contains current corroborating information (e.g., either address of record or nationality of record), OR verification of a financial account number (e.g., checking account, savings account, loan or credit card) confirmed via records.
- The Registration Agent (RA) must inspect the primary photo-ID and verify via the issuing government agency or through credit bureaus or similar databases. The verification confirms that name, date of birth, address, and other personal information in record are consistent with the application. The RA compares the picture to the applicant and records ID number. The Registration Agent inspects the secondary government ID and if apparently valid, confirms that the identifying information is consistent with the primary photo ID, or;
- The Registration Agent verifies the financial account number supplied by the applicant through record checks or through credit bureaus or similar databases, and confirms that name, date of birth, address, and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. The Registration Agent records a current biometric (e.g., photograph, fingerprints) to ensure that the applicant cannot repudiate the application.

[86] FIPS 201-2 now defines it own list of acceptable identity documents and does not mention OMB 115-0136 (Form I-9) anymore. This might create an issue for NFIs issuing PIV-I Cards non-US nationals.

- The Registration Agent issues credentials in a manner that confirms address of record.

In addition to its role in ensuring the validity of an identity card, the PIV-I hardware policy identity authentication PKI certificate ensures that the NFI meets E-authentication assurance level 4 identity proofing. As a result, Federal government relying parties can trust the asserted identity of the NFI PIV interoperable cardholder.

12.2.6.2.2 Background Vetting Process

The Federal background vetting process (e.g., NACI) is performed in order to determine an individual's suitability/fitness to work for or on behalf of the Federal government and is not applicable to NFI identity cards.

For purposes of PIV interoperability, NFIs need to concern themselves only with satisfying the identity proofing requirements for E-authentication Assurance Level 4. Where suitability/fitness is a concern for an agency, the agency may require further background checks for access.

13 Federal PKI, PIV and PIV-I

The Federal government uses public key technology and a public key infrastructure (PKI) to implement strongly authenticated, trusted transactions within a Federal agency, between Federal agencies, and between agencies and external organizations (e.g., business partners, state and local governments, citizens). The growth of PKI was driven by a number of government mandates for electronic authentication.

This section provides an overview of the federal PKI. Detailed information about public key technology and PKI can be found in CSCIP Module 2, *Security*.

13.1 Federal PKI Timeline[87]

Federal PKI implementation started in the 1990s as both government and industry moved to electronic delivery of services and electronic transactions. The emergence of government-wide electronic authentication and identity management guidelines, mandates, and standards has greatly facilitated government-wide interoperability of credentials and PKI adoption. Key mandates and guidance included the following:

- In 1997, Vice President Al Gore published "Access America," a report which outlined actions the Federal government is taking to promote the electronic delivery of services, and electronic transactions between agencies and trading partners, over open networks such as the Internet.[88] The report identified identity assurance/information security as a key enabler for e-Government.
- In 1998, the Office of Management and Budget (OMB) and the Federal PKI Steering Committee, in conjunction with the National Partnership for Reinventing Government, published "Access with Trust," a report describing Federal agency efforts to employ a specific security technology – public key cryptography – which is particularly well suited for achieving authentication, information integrity, non-repudiation, and confidentiality of transactions over open networks. Access with Trust described agency pilot efforts using public key technology, and it set forth certain principles which would guide Federal adoption of this technology: (a) the use of commercial off-the-shelf software to the maximum extent practical; (b) the use of open vs. proprietary standards; (c) a strong bias towards product neutrality – that is, allowing agencies to select whatever products they determine will best suit their needs; and (d) a strong desire to deploy solutions which are interoperable, scalable (having the ability to serve large numbers of users), and extensible (having the ability to serve multiple applications from one infrastructure).Also in 1998, Congress enacted the "Government Paperwork Elimination Act" (GPEA, Public Law 105-277) requiring that when practicable, Federal agencies by October 2003 accept forms electronically with electronic signatures.
- In June 2000, Congress enacted the "Electronic Signatures in Global and National Commerce Act" (the E-Sign Act)[89] to facilitate the use of electronic records and signatures in interstate and foreign commerce by ensuring the validity and legal effect of contracts entered into electronically.
- The Federal PKI Architecture (FPKIA) debuted in 2002 and included the Federal Bridge Certificate Authority (FBCA) and four cross-certified Federal agencies: United States Department of Agriculture (USDA)/National Finance Center, Department of Defense (DoD),

[87] Sources for this section include: "The Evolving Federal Public Key Infrastructure," Federal Public Key Infrastructure Steering Committee, Federal CIO Council, June 2000, http://www.idmanagement.gov/documents/evolving-federal-public-key-infrastructure; "The Realized Value of the Federal Public Key Infrastructure," Identity, Credential and Access Management Sub Committee (ICAMSC), January 29, 2010; "HSPD-12: Defining a Federal PKI Framework," Judith Spencer presentation, Smart Cards in Government Conference, April 2006.

[88] "The Evolving Federal Public Key Infrastructure," Federal Public Key Infrastructure Steering Committee, Federal CIO Council, June 2000, http://www.idmanagement.gov/sites/default/files/documents/pki-brochure.pdf

[89] http://www.ftc.gov/os/2001/06/esign7.htm

Department of the Treasury (Treasury), and National Aeronautics and Space Administration (NASA). The FBCA enabled interoperability of disparate agency PKIs. The FBCA continues to operate under the management of the General Services Administration (GSA) with policy oversight provided by the Federal Public Key Infrastructure (FPKI) Policy Authority (FPKIPA). Today, the FBCA's primary role is to enable interoperability between FPKI domains, and to enable Federal interoperability with non-Federal PKIs.[90]

- In July 2003, the Office of Management and Budget (OMB) memorandum, "*Streamlining Authentication and Identity Management within the Federal Government*"[91] instructed Federal agencies to "buy-not-build" PKI to the maximum extent possible.
- In December 2003, OMB issued memorandum M-04-04, "E-Authentication Guidance for Federal Agencies," which established four levels of identity assurance for the authentication of electronic transactions. Levels of assurance 3 and 4 require PKI support.
- Homeland Security Presidential Directive 12 (HSPD-12), signed by President Bush in August 2004, set the policy for a common identification standard for Federal employees and for contractors who are conducting business with Federal agencies and who require access to physical and information technology (IT) resources.
- OMB memorandum M-05-05, "Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services,"[92] published December 20, 2004, identifies the Shared Service Provider (SSP) Program as a source for Federal agencies to obtain PKI services. The SSP Program provides strong government oversight of commercially-managed service providers, which results in cost savings, benefits associated with contractor-provided services, and risk mitigation. In addition, the SSP Program ensures PKI services consistent with current electronic signature law and policy.[93]
- In February 2005, in response to HSPD-12, NIST Computer Security Division developed FIPS 201 and, subsequently, SP 800-73, to define the technical requirements and specifications for a common identity credential. FIPS 201 requires PIV cards to contain PKI-based authentication data (at least one asymmetric key pair and one corresponding digital certificate) for high-confidence physical and logical access to Federal facilities and systems.
- In August 2013 NIST published the revised version of FIPS 201. This new version (FIPS 201-2) introduces some new concepts (e.g., On Card Comparison for biometrics, use of the contactless interface with a secure messaging session), as well as changes in the options (or requirements) in the PIV data model (e.g., CAK and Card UUID mandatory, optional Cardholder UUID).
- As of December 1, 2013, over 4.66 million HSPD-12 credentials are used by Federal employees (96% of the total population) and over 1 million credentials are used by contractors.[94]

The result of these mandates and subsequent program initiatives has been broad use of PKI across the Federal government and with government business partners and increasing use of PKI by commercial organizations and state and local governments.

[90] Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, "The Realized Value of Federal PKI.", http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf
[91] http://www.whitehouse.gov/sites/default/files/omb/inforeg/eauth.pdf
[92] http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-05.pdf
[93] "The Realized Value of Federal PKI," op. cit.
[94] *hspd-12_reporting_workbook_status_report_q1fy2014.pdf*

13.2 The Federal PKI Landscape

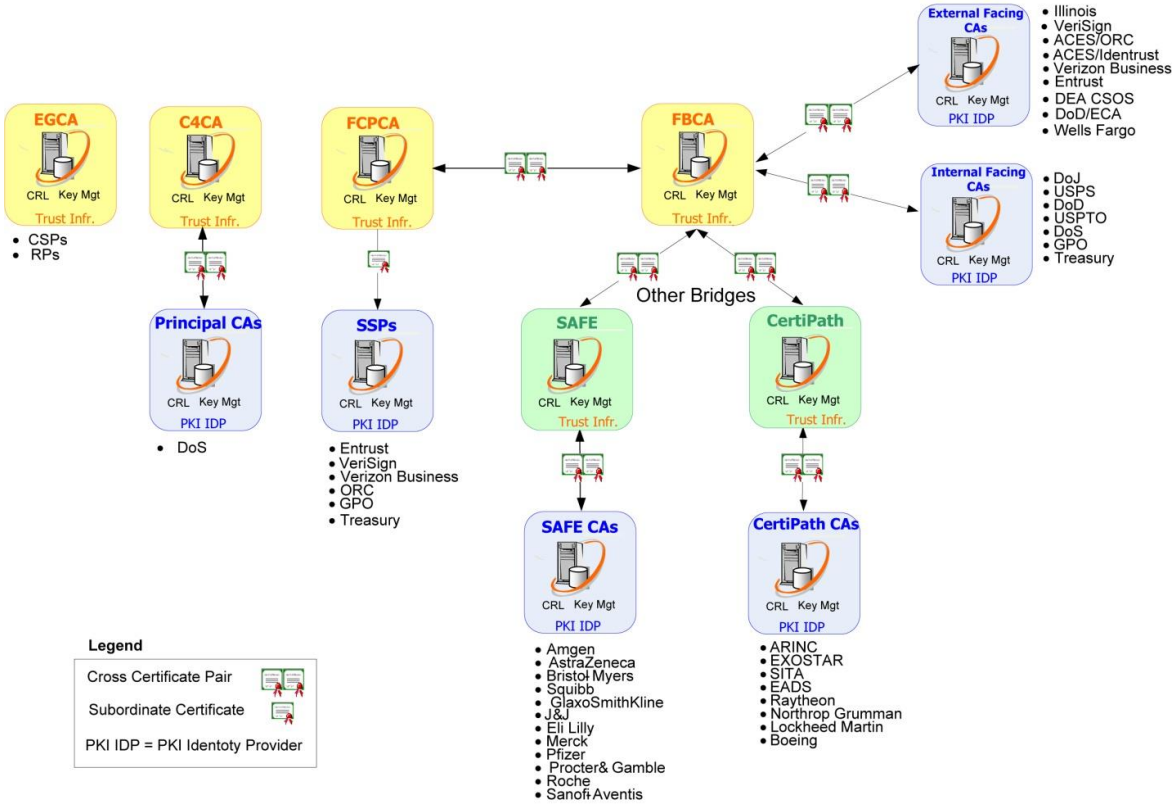
Note: The following section was extracted from the Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, "The Realized Value of Federal PKI."[95]

13.2.1 The Federal Public Key Infrastructure (FPKI)

The FPKIPA develops Federal PKI policy and provides operations oversight. The FPKIPA is an interagency body established under the Chief Information Officers (CIO) Council to enforce digital certificate standards for trusted identity authentication across Federal agencies, and between Federal agencies and outside bodies such as universities, state and local governments, and commercial entities. The primary FPKIPA mission is to provide a solution for strong authentication, digital signature capability, and confidentiality for data in transit and data at rest.

Figure *10* depicts the current FPKI[96]. The FBCA and Federal Common Policy CA (FCPCA or COMMON) are cross-certified with each other, while the E-Government Certification Authority (EGCA) and Citizen and Commerce Class Common Certification Authority (C4CA) stand alone.

Figure 10. FPKI Landscape, September *2009*



[95] "The Realized Value of Federal PKI," Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, January 29, 2010, http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf

[96] As of January 2010, Entrust and Verizon Business were not yet cross-certified with the FBCA. However, in anticipation of their cross-certification, they were included in the ICAMSC white paper. Entrust was certified by DoD on February 2010 and Verizon Business was certified on October 2009.

13.2.1.1 Federal Bridge Certificate Authority (FBCA)

Originally developed as a mechanism to facilitate interoperability between Federal agency enterprise PKI implementations, the FBCA's role has subsequently expanded to include external entities. Today, the FBCA is the identity trust hub that enables peer-to-peer transactions among its member organizations, both Federal and non-Federal.

Federal agencies operating PKIs cross-certified with the FBCA are[97]:

- Department of Defense (DoD);
- Department of State (DoS);
- Department of Justice (DoJ);
- Department of Energy (DOE);
- National Institute of Standard and Technology (NIST);
- Health and Human Services (HHS);
- Environmental Protection Agency (EPA);
- Federal Election Commission (FEC);
- Federal Trade Commission (FTC);
- Department of Transportation (DOT) /Federal Aviation Administration (FAA);
- Department of Homeland Security (DHS);
- National Aeronautics and Space Administration (NASA);
- Social Security Administration (SSA);
- Department of Veteran Affair (VA);
- Executive Office of the President ;
- Drug Enforcement Administration (DEA CSOS);
- Government Printing Office (GPO);
- Department of Treasury (Treas);
- United States Postal Service (USPS); and
- United States Patent and Trademark Office (USPTO).

The FBCA is also cross-certified with the State of Illinois, and with two commercial PKI bridges: CertiPath, which serves the aerospace and defense industry, and SAFE-BioPharma, which has established FBCA-comparable digital identity and signature standards for the pharmaceutical and healthcare industries. These partners have extended the reach of the FPKI well beyond its own boundaries. In addition, there are PKI service providers associated with the FBCA: Access Certificates for Electronic Services (ACES), for which GSA administers the Certificate Policy; and Digicert, Identrust, ORC, Symantec/VeriSign, Entrust, Exostar and Verizon Business, which are commercial service providers offering Federally-trusted credentials to U.S. state and local governments as well as business entities.

13.2.1.2 E-Government Certification Authority (EGCA)

To support levels of assurance 1 and 2, the FPKIPA developed the 'X.509 Certificate Policy for the E-Governance Certification Authorities"[98]. The EGCA issues PKI certificates to approved credential service provider (CSP) and Federal relying party (RP) systems to enable mutual authentication, and therefore mutual trust. These credentials establish secure communication links between recognized and trusted entities. Since only approved CSP and RP applications have EGCA credentials, the ability for a non-trusted entity to impersonate either identity or intercept the transaction is eliminated.

[97] Source is a combination of Http://iase.disa.mil/pki-pke/interoperability/pages/index.aspx and http://www.idmanagement.gov/entities-cross-certified-federal-bridge

[98] http://www.idmanagement.gov/fpkipa/documents/EGovCA-CP.pdf

The EGCA supports the ICAM mission by[99]:

- Enabling governance – control which endpoints participate and can be trusted for technical interoperability or information sharing.
- Conveying trust between endpoints in a transaction – allow endpoints to determine trust at run time.
- Facilitating secure communications between endpoints in a transaction – once endpoints have established trust, the ensuing communication between endpoints is secure.

The EGCA supports ICAM assertion-based initiatives:

- Issues certificates to devices and applications.
- Issues different types of certificates to different types of endpoints.

The EGCA Enables trusted access to government services for more participants and communities of interest (e.g., commercial and financial communities).

13.2.1.3 Federal Common Policy Certificate Authority (FCPCA or COMMON)

In April 2003, the CIO Council challenged the FPKIPA to establish an FPKI hierarchical trust anchor for all Federal agency CAs. The resulting "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework" document[100] and the instantiation of the COMMON Root CA represented the beginning of a new era in FPKI. On July 3, 2003, OMB released the policy memo "Streamlining Authentication and Identity Management within the Federal Government," which advised Federal departments and agencies to cease building enterprise PKI solutions and to acquire PKI services from commercial providers. Commercial SSPs were invited to apply for subordination to COMMON via Certification Practices Statement (CPS) mapping to the COMMON certificate policy (CP). Departments and agencies were then free to acquire services from one of these approved providers. COMMON provides a single trust anchor for Federal PKI transactions and interfaces with the external trusted PKI communities through a single cross certification between COMMON and the FBCA.

COMMON enhances the FPKI as follows:

1. Federal agencies can deploy digital credentials without having to operate and maintain an enterprise PKI. Instead, they can acquire services from commercial providers, thus saving their resources for Federal agency purposes.
2. Individual Federal agencies are relieved from the requirement to establish their own CPs and to map to the FBCA. On their behalf, the FPKIPA administers COMMON and manages cross-certification with the FBCA.
3. COMMON is the single trust root supporting interoperability within the Federal government. And because it is cross-certified with the FBCA, it enables public trust of government-issued certificates.
4. COMMON is public facing and has its root CA in an increasing number of COTS product trust stores. This facilitates path discovery and validation because the route between the trusted pairs is more direct than when traversing the FBCA.
5. FIPS 201 identifies COMMON as the source of digital authentication certificates for the PIV credentials.

[99] Text extracted from a presentation done by Judy Spencer in January 2014 at the Office of the National Coordinator for Health IT.

[100] http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf (Version 1.17, December 2011)

13.2.1.4 Citizen and Commerce Class Common Certificate Authority (C4CA)[101]

The C4CA, which is operated by the GSA under the auspices of the FPKIPA, defines the minimum set of requirements for certificates (trust path creation and verification of digital certificates) accepted by the U.S. Federal government for the purpose of authenticating citizens and commercial enterprises for many electronic services. C4CA is the U.S. Federal government's mechanism for enabling a PKI trust domain satisfying level of assurance 2. Its primary purpose is to ensure that "commercial grade" PKI implementations (e.g., those that do not aspire to the requirements for FBCA cross-certification) are not disenfranchised as identity solutions. Uptake of C4CA is somewhat limited. However, DoS has been approved for cross-certification with C4CA in anticipation of extending electronic services to citizens without commingling certificates with employees.

13.2.2 Legacy FPKI Participants

A "legacy FPKI" is a Federal agency PKI operated and maintained by a Federal agency and directly cross-certified with the FBCA, as opposed to obtaining PKI services and credentials from an SSP under COMMON. Current legacy FPKIs are DoS, DoJ, DoD, Treasury, USPS, USPTO, and GPO. These Federal agencies were early adopters of PKI whose systems pre-date the issuance of the 2003 OMB Memorandum requiring the use of shared providers.

As the government-wide initiative for identity management evolves and in order to comply with the requirements of FIPS 201, legacy FPKIs must evolve to remain in step. In this vein, legacy FPKIs have taken steps to conform to FIPS 201 requirements in order to align themselves for the purpose of issuing PIV Authentication certificates. Towards this end, COMMON includes provisions specifically developed to ensure legacy FPKI implementations can be aligned (e.g., naming conventions). In addition, there are plans to transition legacy FPKIs from the FBCA to a direct peer-to-peer relationship with COMMON in order to further simplify trust paths within the Federal community.

13.2.3 External FPKI Partners

Currently, external FPKI partners associated with the FBCA include one state and two industry PKI bridges. In 2003, the State of Illinois became the first external entity to cross-certify with the FBCA.

However, it was the addition of the two commercial PKI bridges that significantly increased the FBCA external trust community.

13.2.3.1 CertiPath

CertiPath is a commercial standards-based PKI bridge establishing interoperable trusted identity credentials within the aerospace and defense (A&D) industry. CertiPath certifies organizations to a common standard, enabling them to assert the identities globally – utilizing software-based digital certificates or certificates deployed on hardware tokens – such as smart cards – to gain logical access to sensitive intellectual property and physical access to secure locations and corporate offices. The CertiPath Bridge gives receiving organizations the confidence of knowing that the individual identities conveyed by their partners have at least the same level of assurance as those asserted by their own employees.

CertiPath provides externally portable organizational and individual identity assurance by certifying an organization's credentials – and those of its employees – meet the same globally accepted standards. CertiPath maps an organization's policy to the CertiPath policy to ensure adherence to the standards, essentially providing a trusted "seal of approval."

CertiPath was designed to be a geopolitically neutral mechanism, meeting globally accepted standards for Certificate Policies (CPs) and interoperability.

[101] Reference document: http://www.idmanagement.gov/sites/default/files/documents/citizen_commerce_cp.pdf

In addition, the CertiPath Certified Credential Provider (3CP)™ program offers certification of Service Provider CAs who can, in-turn, issue certificates to enterprise customers at levels of assurance that match their certification with CertiPath. There are three companies who are 3CP™ certified: Citibank, EXOSTAR, and SITA.

Through its certification with the FCBA, CertiPath allows A&D contractors to conduct highly secure business communications with the Federal government. Current CertiPath member CAs include Citibank, EXOSTAR, SITA, EADS, Raytheon, Northrop Grumman, Lockheed Martin, and Boeing.

13.2.3.2 SAFE-BioPharma Association PKI Bridge

SAFE-BioPharma™ is a non-profit association that developed and manages digital identity and signature standards for the pharmaceutical and healthcare industries. Organizations seeking to provide authentication and digital signature services and to become issuers of SAFE-BioPharma credentials must first cross-certify with the SAFE-BioPharma Bridge CA.

Current SAFE-BioPharma member CAs include: Amgen, AstraZeneca, Bristol-Myers Squibb, GlaxoSmithKline, Johnson & Johnson, Eli Lilly, Merck, Pfizer, Procter & Gamble, Roche, and Sanofi-Aventis.

13.2.3.3 State of Illinois

In 2003, the State of Illinois became the first non-Federal entity to cross-certify with the FBCA. The State of Illinois provides full PKI services to its constituents, including strong authentication, digital signatures, and encryption services. This includes encrypted background checks for schools, digitally signed water discharge monitoring forms from the Environmental Protection Agency, strong authentication to Medicaid recipient information, and digitally signed forms at a municipal police department.

Illinois is the first non-Federal government entity to be cross-certified at the medium-hardware level of assurance with the FPKI. This will allow for the issuance of the First Responder Authentication Credential (FRAC) (following the PIV-I guidance[102]) to first responders within Illinois. Using these strong authentication credentials, Illinois first responders (e.g., police, firefighters, paramedics) will have up-to-date identification which will allow them quick access to emergency or disaster sites. In addition, the check-in agent at the site will be able to review not only the cardholder's identification information, but also training information, certifications held, and licenses the holder possesses. In this way, the responders will be allowed access to the site and directed to where they can be of the greatest assistance. Since these credentials follow the guidelines of the Department of Homeland Security (DHS), the expectation is that they would be accepted nationally when Illinois sends volunteers to assist at incidents in other jurisdictions.

13.2.4 SSP PKI "Clones"

PKI SSPs offer out-sourced FPKI and COMMON services to Federal agencies. Per COMMON, SSPs cannot use this relationship with COMMON to sell credentials to non-Federal entities in order to attain a trust relationship with the FPKI. As a result, several commercial providers approved as SSPs under COMMON have elected to cross-certify with the FBCA for the purpose of issuing certificates to external entities that can be trusted by the Federal community. The FPKIPA refers to these services as commercial "clones" of the SSP offering.

The first responder community (with FRAC) and the transportation/port worker community (with Transportation Worker Identification Credential, or TWIC) are two such external entities desiring a PKI-based trust relationship with the Federal government. This interoperability with external entities via SSP "clones" is expected to grow as more organizations adopt public key solutions and seek relationships with the Federal community.

[102] See http://info.idmanagement.gov/2012/06/new-ficam-guidance-on-using-piv-and-piv.html or http://www.idmanagement.gov/sites/default/files/documents/PIVI_Certification_Process.pdf

13.2.5 Partnership with Academia

The FPKI has a research partnership with the higher education community, sponsored by EDUCAUSE, a non-profit organization whose mission is to advance higher education by promoting the intelligent use of information technology. The Higher Education Bridge CA (HEBCA) is a test CA housed at Dartmouth College.

13.2.6 The Four Bridges Forum

The nation's four leading PKI bridges have joined forces under a federation called the Four Bridges Forum (4BF). Its purpose is to raise awareness and promote use of a growing global infrastructure that enables trusted transactions across diverse communities of interest. 4BF includes the FBCA, CertiPath, the SAFE-BioPharma Association, and HEBCA.

13.3 The Value of PKI to the Federal Government

Note: The following section was extracted from the Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, "The Realized Value of Federal PKI."[103]

This section discusses PKI qualitative and quantitative benefits to both Federal agencies and cross-certified external PKIs.

13.3.1 Qualitative Benefits of PKI

13.3.1.1 Strong Digital Signatures

Public key technology is based on asymmetric key exchange. This means that each holder of a PKI credential has a unique key pair, one of which is kept secret (the private key) and the other of which can be shared (the public key). The private key is used by the credential holder to create signatures for documents and to assert identity during an attempt to gain access. The public key is then used by the relying party to verify the authenticity of the signature or the identity claim. The private key remains in the control of the credential holder and cannot be determined from the public key, thereby preventing spoofing. The trust in the identity asserted in the asymmetric key exchange process is provided by the strength of the binding between the public key and the identity asserted by its certificate. This binding is the responsibility of the public key infrastructure (PKI), the set of policies and procedures that govern the determination of identity and the binding of that identity to the public key. The FPKI policies provide a single consistent framework for trusting public key certificates within the Federal community and between the Federal government and its external partners.

The algorithms used to create digital signatures using public key technology are under constant attack, as are the keys themselves. For this reason, the size (length) of keys and the algorithms used to manipulate them is subject to constant review and refresh. NIST Special Publication 800-57, "Recommendation for Key Management,"[104] requires that key lengths in use by Federal agencies provide a minimum of 112 bits of security strength (this requires a 2048-bit key for RSA) and the use of secure hash algorithm (SHA-2) for performing cryptographic hash functions[105]. These requirements are reflected in FPKIPA policies.

In addition to the strength of the algorithms, the method of storage for the private keys contributes to the level of trust that can be placed in a transaction. Private keys can be stored in either software-based or hardware-based modules. Hardware-based private key storage provides better security and portability,

---

[103] "The Realized Value of Federal PKI," Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, January 29, 2010, http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf f

[104] NIST Special Publication 800-57 (SP 800-57, "Recommendation for Key Management," Revision 3, July 2012, http://csrc.nist.gov/publications/PubsSPs.html

[105] SP800-57 Part 1 revision 3 requires the use of algorithms providing minimum security strength of 112 bits until 2030 and requires 128 bits for 2031 and beyond.

which contribute to credential strength, and is not subject to the attacks that can undermine software-based modules. Hardware modules can take many forms, including smart cards, USB tokens, and smart phones.

When used within a federated model, digital signatures allow important business and regulatory transactions to occur in a fully electronic, secure environment. This eliminates the need to handle, copy, ship, and store paper documents. An example of the cost savings and enhanced security is the Federal government's transition to paperless processing. Federal government use of digital signatures to sign PDF files is widespread, as exemplified by the GPO. Use of PKI features such as digital signature is especially pertinent for digital-only content. The increasing demand from the Federal government is driving increased support for stronger algorithms in COTS products.

13.3.1.2 Support for Technical Non- repudiation

The use of digital signatures by the FPKI community supports legally-recognized technical non-repudiation (i.e., someone claiming that he or she did not sign). When a document is "digitally signed," the document's contents are incorporated into the signature. In order for the "signature" to validate, not only must the relying party use the public key that corresponds to the signer's private key[106], but in addition, the content of the document must not have changed since the signature was affixed. Digital signatures function as a unique identifier for an individual, much like a written signature, and also validate the contents of the signed document, which a written signature cannot do.

Legally speaking, technical non-repudiation requires a chain of evidence that links the individual to the signed document. PKI supports this requirement in two ways: first, only the individual whose private key corresponds to the public key used to validate the document can have signed the document, and second, successful validation indicates that the document contents were not tampered with subsequent to the application of the signature.

Digital signatures remain legally vulnerable to non-technical repudiations such as lack of legal capacity to contract (e.g., mental state) and forced/unintended signature (e.g., forced to sign, accidentally hit the "sign" button).

13.3.1.3 Strong Authentication

PKI credentials can be used in place of traditional forms of identity assertion (e.g., userid/password) in order to strengthen the access control process. In this case, the digital signature process is part of a challenge/response process. The access control system has a record of all PKI certificates and corresponding public keys whose owners are permitted access to the system or facility. When the individual attempts to gain access (either by logging on to a system or network, or approaching a physical access terminal), a challenge is presented, which is signed using the individual's private key. This signed challenge is verified using the stored public key and current certificate revocation list. If verification is successful, the individual's asserted identity is accepted, and access is granted.

New accounts are easily created by adding public keys and PKI certificates to the access control system. In the case of visitors carrying PKI certificates on their identity credentials, the PKI certificates can be validated to determine they were issued by a recognized authority and have not been revoked for any reason. In addition, a challenge/response process can verify that the credential carries the private key that corresponds to the public key associated with the PKI certificate, a process that requires the credential holder to activate the private key using an access PIN, which comprises a two-factor access control activity: something you have, something you know. Finally, this information can be used to request additional identity information through an attribute exchange mechanism. Using the capabilities of public key technology and infrastructure, credentials are validated readily as part of the access decision-making process.

[106] This verification requires not only a validation of the private key certificate, but also includes a complete path validation to a common root of trust, making sure the other party is trusted and nothing in the chain of trust was repudiated.

An example of a strong authentication and access control mechanism that takes advantage of the capabilities of public key technology is the government-wide PIV Card mandated by HSPD-12, and its embedded PIV Authentication Key, whose use and authority is governed by the Federal Common Policy Framework. The PIV Card puts strong hardware-based authentication processes in the hands of every Federal employee and contractor. The recently released PIV Interoperability for Non-Federal Issuers guidance offers similar strong authentication capabilities and mutual trust to communities external to the Federal government through the federated environment.

13.3.1.4 Strong Encryption

Encryption is used to protect data at rest (e.g., computer hard drives, storage devices) and data in motion (e.g., transmission over the Internet, e-commerce, mobile telephones, e-mail). Traditional encryption processes use symmetric keys which must be shared in advance among all authorized entities in order to gain access to encrypted data. Therefore, symmetric keys must be kept well protected in order to protect the integrity of the encrypted data. When using PKI for encryption purposes, there are two distinct processes that may be implemented. In the first, the data is encrypted with the public key of the individual for whom it is intended. Once encrypted in this manner, it can be decrypted only with that individual's private key. In the second, the PKI is used as part of the process to securely share and store a symmetric key that is used to encrypt and decrypt the data. In both cases, the ability to access or compromise the key used to decrypt the information is greatly reduced.

Generally, the size of the cryptographic keys contributes to stronger encryption. Complying with technical standards and best practices for ensuring the continued strength of its encryption processes is the reason for FPKIPA replacement of 1024-bit keys with 2048-bit keys. Federal agencies are using PKI not only in the process of encrypting and decrypting data files, but also to compress and decompress those same files for transmission.

13.3.1.5 Trusted Interoperability between Disparate Systems

Organizations generally use unique internal policies and procedures to manage the identities of their employees and collaborating groups. These policies and procedures do not easily or efficiently align with the policies and procedures used by other organizations.

Federated PKI trust mechanisms, such as the FBCA and the other bridges that are partnering with it, allow trusted interoperability among disparate systems, greatly facilitating e-Commerce. The bridges negotiate common ground among the organization-unique internal policies and procedures, which in turn enables recognition, mutual trust, and acceptance of each other's identity credentials. And because the PKI credential is unique to its owner, not requiring shared secrets or other exchange of information, this inter-organizational trust is readily extended to all individual credentials within a federated organization, whether used to enable secure e-mail exchange, digital signature, or access control activities. In this manner, CertiPath promotes interoperability between the aerospace industry and DoD over the Internet through use of its PKI bridge's relationship with the FBCA.

For the Federal community, the move to the COMMON trust root for PIV cards has simplified the cross-organizational trust model, since all trust has been placed in the single policy and its certification authority. The COMMON trust root has been added to commercial product root stores further facilitating federated trust. The FPKI is also working with the other major browser organizations to install the COMMON trust root in their trust stores. This will further facilitate inter-organizational trust, both within the Federal community and between the Federal community and its external partners.

13.3.2 Quantitative Benefits of PKI

It is generally believed that an accurate determination of PKI return on investment (ROI) is difficult because effective PKI implementations are tightly integrated within larger business systems and processes. Therefore, it may be impossible to differentiate the ROI directly attributable to the use of PKI from the ROI of the overall system's effectiveness. However, it is helpful to quantify PKI ROI in terms of

a) increased protection for government assets, b) greater efficiencies in doing business, and c) reduced costs. It can be demonstrated that improving trust in the Internet for the exchange of sensitive information results in lower cost, more streamlined communications, and accelerated process improvements, in part because digital transactions vastly reduce paper use.

For example, DoS has seen drastic reductions in help desk management costs by reducing its use of passwords in favor of PKI-enabled logical access control. For CY2002 through CY 2008, DoS has saved $8 million in password management costs.

Another example is the Department of the Treasury's PKI, which is used at many bureaus, including Departmental Offices (DO), Bureau of Engraving and Printing (BEP), Bureau of the Public Debt (BPD), Financial Management Service (FMS) and the U.S. Mint. Collectively, the Treasury PKI is used to protect trillions of dollars per year by providing strong authentication, encryption and digital signature services to mission-critical applications such as the FMS Secure Payment System.

13.3.2.1 Synergy with HSPD-12[107]

The HSPD-12-driven, large-scale issuance of PIV cards to all Federal employees and contractors will make Federal government use of PKI more prevalent. At the end of fiscal year 2009, the deployment of PIV cards across the Federal enterprise exceeded 60% of the workforce, with 22 Federal credential issuance infrastructures operational nationwide and multiple industry participants on the GSA Approved Products List. By December 1st 2013, 95.3% of the Federal work force (employees, contractors and guest researchers) had been provided with a PIV Card.

In practice, PIV cards are issued with the mandatory PKI credential, the PIV authentication key, and since FIPS 201-2, the three other PKI credentials: card authentication key, digital signature key, and key management (encryption) key. It is expected that, in the future, all Federal users will be supplied with PKI credentials via the PIV card. This ubiquity will enable large scale implementation of PKI-enabled solutions for access control, data protection, and business process streamlining; and will result in greater logical and physical security for employees and contractors throughout the Federal government. Including PKI in the PIV initiative may be the single most important security enhancement in the history of the Federal government.

13.3.2.2 Multi-factor Authentication

Authentication systems are often categorized by the number of factors that they incorporate. PKI is an excellent component (factor) to multi-factor authentication.

PKI can contribute several factors. By default, PKI contributes something you have (the private cryptographic key). If the PKI software or hardware module housing the private key requires user activation, PKI also contributes either something you know (a password to unlock the module in order to access the private key) or something you are (a biometric to unlock the module to access the private key[108]). Federal agencies are leveraging this multi-factor approach, typically using a password to unlock the software or hardware module to gain access to the PKI private key.

13.3.2.3 Network Security

13.3.2.3.1 Access Control

PKI-based authentication is becoming widely used as a primary factor for access control to critical Federal agency resources. This will become ubiquitous as HSPD-12 deployment and implementation increases. Today, the best metric indicating the value of PKI for network security is from DoD. DoD reports reduced network intrusion and penetration attacks where PKI is used in conjunction with the DoD

[107] This section, initially extracted from the document written on January 2010 "RealizedValueFederalPKI.pdf" has been edited to reflect more recent numbers.

[108] This feature is now possible with FIPS 201-2 PIV cards using the optional OCC user authentication method.

Common Access Card (CAC). In an environment where one successful attack could cost tens of millions of dollars, the potential cost savings is significant.

> "CCL [CAC Cryptographic Logon (CCL)] implementation across DoD has resulted in a 46% reduction in successful NIPRNet intrusions," according to Lt Gen Charles Croom, Director, DISA and Commander, Joint Task Force-Global Network Operations at the AFCEA SpaceComm 2007 Conference."

13.3.2.3.2 Secure Tunneling

The FPKI community is benefiting from using PKI to secure communications, such as virtual private networks (VPNs). VPNs use PKI certificates to establish a secure tunnel through which data can be transmitted across a public network, such as the Internet, without being subject to threats such as eavesdropping. By using secure tunneling, organizations avoid the risk and costs of data tampering or data theft during transmission.

The SAFE community, exemplified by Johnson and Johnson (J&J), also uses two-factor authentication (something you have, i.e., smart card-based PKI credential; something you know, i.e., access PIN) to authenticate to the network and create an Internet Protocol Security (IPSec) tunnel. Tunneling protocols may use data encryption to transport unencrypted (i.e., plain text) traffic over a public network (e.g., Internet) through an encrypted channel, thereby providing VPN functionality. IPSec has an end-to-end Transport Mode, but also can be operated in a Tunneling Mode through a trusted security gateway.

13.3.2.3.3 Single Sign-on

Single sign-on (SSO) allows a user to log in once and gain access to multiple independent systems (possibly with different authentication mechanisms) without being prompted to log in again at each of them. Single sign-off is the reverse property whereby a single action of signing out terminates access to multiple systems. Using public key technology for achieving SSO applies a strong two-factor identifier (PKI credential and its activation PIN) to the process. Once activated for an SSO session, the PKI credential can conduct the authentication activity for accessing additional resources on the network without additional user intervention. PKI does not operate the way industry defines SSO, but provides all the user benefits of SSO without requiring the extensive back-end coordination that traditional SSO solutions require. In addition, the use of PKI eliminates the need for ever-increasingly complicated passwords that must be changed at increasingly shortened intervals. SSO benefits utilizing PKI include:

1. Eliminating password fatigue (i.e., having to remember too many different user name and password combinations);
2. Reducing time spent re-establishing identity for the same individual;
3. Reducing IT costs by eliminating IT help desk calls concerning passwords;
4. Eliminating vulnerabilities associated with large password databases;
5. Security on all levels of entry/exit/access to systems without the inconvenience of re-prompting users; and
6. Centralized reporting for compliance adherence.

13.3.2.3.4 PKI-enabled Applications

PKI-enablement of applications is occurring in internal, intranet-based, and Internet-based environments. The types of interactions vary greatly, from signing and encrypting e-mail, to access control processes. Once enabled, an application is able to process any public key certificate it receives and make a trust decision without relying on end-user cognizance. In addition to examining the PKI certificates for content and expiration date, PKI enablement includes the capability to perform trust path discovery and validation. This is the process of tracing the PKI certificate's origins and relationships to determine whether it should be trusted. The goal is an unbroken chain of trust from the relying party to the issuing entity. Additionally,

PKI-enabled applications must perform certificate revocation checking to determine the specific certificate's current validity (i.e., it has not been revoked by the issuer prior to its expiration date).

An example is the GPO PKI-enabled the Office of Federal Register electronic submission system (eDOCS). This provides significant benefits to submitting Federal agencies by avoiding courier charges and reducing cycle times. Federal agencies that submit large numbers of Federal Register announcements via the PKI-based electronic submission method can recoup costs within three to six months. In addition, PKI-enabled electronic submission provides a significant benefit to Continuity of Operations (COOP), whereby electronic documents can be easily replicated and sent to disaster recovery command centers instantly in contrast to paper documents that need to be copied and couriered to a disaster recovery site.

Another example is DoS PKI-enablement of the Consular Affair's Adoption Tracking Service and the Immigrant Visa Allocation Management System (IVAMS). This PKI-enablement of an Internet-based application provided DoS an annual cost savings of over $700,000 compared to the paper-based, manual processes previously employed. Not only did it reduce man hours, but it decreased the time to respond to the request from days to seconds.

13.3.3 Case Studies

In March 2009, the FPKIPA asked its cross-certified members, including the CertiPath and SAFE Bridges, to provide ROI and other qualitative and quantifiable data on the realized value of FPKI within their organizations.

Currently, eight Federal agencies operate their own PKIs: DoD, DEA, DoS, Treasury, GPO, DoJ, USPTO, and USPS. Four Federal agencies implemented their own PKIs, but subsequently acquired PKI services from SSPs. Other Federal agencies either acquire their public key certificates from the SSP program or they have an internal PKI that does not issue certificates outside the Federal agency.

Table 14 is a consolidated summary of qualitative and quantitative benefits realized by cross-certified members. The solid black dots indicate where a cross-certified member is benefiting from PKI use. Dollar signs indicate where the member provided financial impact information, either in dollars, percentages, or orders of magnitude. Benefits are grouped (e.g., network security encompasses strong authentication for access control, SSO, and VPN usage) into major areas of benefit.

Additional detail on the case studies can be found in the ICAMSC white paper, "The Realized Value of PKI."

Table 14. Qualitative and Quantitative Benefits of FPKI[109]

	Qualitative Benefits						Quantitative Benefits				
Cross-Certified Member	Strong Digital Signature	Support for Technical Non-Repudiation	Strong Encryption/ Decryption	Authentication	Interoperability	Network Security	Synergy with PIV	Multi-Factor Authentication	PKI-enabled Applications	Reduced Costs & Greater Efficiency	Multiple Levels of Security
CertiPath	●	●	●	●	●	●	NA		●	●	●
DoD	●	●	●	●	●	$●	●		●	●	●
DoS	●	●	●	●	●	$●	●	$●	$●	●	●
GPO	●	●	●	●	●		$●			●	●
SAFE (J&J)	●					●	NA				
State of Illinois	●	●	●	●			NA	Soon	●	$●	
Treasury	●		●	●	●	●			●		

13.4 The Future of PKI – PIV, PIV-I and Industry Directions

Note: The following section was extracted from the Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, "The Realized Value of Federal PKI."[110]

The future of PKI is closely tied to the increased emphasis on identity management and cyber security both by industry and government. As organizations become more conscious of their cyber security needs, they increasingly recognize the value of public key solutions for providing the technology to attain their identity management and data security goals.

The inclusion of public key credentials on PIV cards ensures that there is widespread availability of these basic tools for strong identity assurance and data protection within the Federal government.

The extension of trusted identity credentials to state and local governments through the DHS-sponsored FRAC and TWIC programs has raised interest in public key solutions in other state and local electronic business activities.

In addition, the adoption of public key technology within industry is becoming more widespread. In many cases, this interest has been generated by the high-level of interest in the FIPS 201 standard for PIV cards and the desire to have identity management processes that are interoperable with Federal systems. The recently released *PIV Interoperability for Non-Federal Issuers* document, providing guidance to non-Federal entities on achieving technical interoperability and trust with Federal systems designed to utilize PIV cards, will further expand PKI credential ubiquity to state and local governments, industry, and commercial activities.

Wide PKI acceptance is also evident in the Federal CIO Council's recent action to create a superstructure comprised of key Federal government identity management initiatives that previously worked independently. These initiatives and their underlying technologies have matured and converged. Combining them under one superstructure – called Identity, Credential and Access Management (ICAM)

[109] "The Realized Value of Federal PKI," Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, January 29, 2010, http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf

[110] "The Realized Value of Federal PKI," Identity, Credential and Access Management Subcommittee (ICAMSC) white paper, January 29, 2010, http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf

– facilitates a clear, consistent, unified picture of where Federal government identity management wants to go. Within this superstructure, PKI plays a prominent role as a provider of strong identity credentials.

Use of PKI outside the Federal government is increasing at a steep rate, as evidenced by the advent of new bridge communities exemplified by the SAFE-BioPharma community and the CertiPath-supported Transglobal Secure Collaboration Program (TSCP), a consortium of the aerospace industry in Europe and the U.S[111].

Increased industry adoption is illustrated by the PKI capabilities embedded in COTS products. Such PKI visibility, prevalence, and scalability will continue to improve the PKI value curve over time because users will be able to readily and seamlessly take advantage of PKI. In time, PKI functionality will be ubiquitous, and therefore more accessible and tangible.

The incorporation of PKI into COTS products is an easy decision for developers because PKI is low risk to implement while providing high value-add. Embedding PKI into COTS products and utilizing it to secure VPNs and implement SSO, affords higher levels of security than riskier technologies that use passwords or PINs. In the future, COTS products based on open standards will incorporate PKI to support digital signature and encryption used to construct trusted message exchanges.

Currently, PKI is integrated into the following:

1. E-mail clients (digitally signing and encrypting e-mails);
2. Form signing software (digitally signing forms);
3. Root stores of major Internet browser and products;
4. Word processors and readers;
5. Internet browsers; and
6. Smart identity cards (e.g., DoD CAC, PIV card, FRAC, TWIC) that move PKI into the physical and logical access control arenas.

The future PKI value curve will be steeper because PKI capabilities are becoming more accessible to more users through ubiquitous applications like browsers and word processors. In addition, interoperable industry infrastructures such as 4BF and TSCP will further steepen the PKI value curve. More use in industry makes it easier for the Federal government to realize more value.

[111] TSCP government members include: U.S. Department of Defense, U.S. General Services Administration, U.S. Secret Service, NASA, French ANSSI, UK Ministry of Defense and the Netherlands Ministry of Defense. Complete list of members at https://www.tscp.org/about-tscp/tscp-members/

14 Federal Identity, Credential and Access Management Guidelines[112]

The Federal Government is operating in a constantly shifting threat environment and identity management issues have been well-documented by the Government Accountability Office (GAO), National Science and Technology Council (NSTC), Office of Management and Budget (OMB). The Administration has laid out clear goals to make government more accessible to the American public and outlined these goals in the new Cybersecurity Initiative.[113] The Open Government Initiative[114] promotes transparent, collaborative and participatory government that fully engages the public, while promoting data security, privacy and high assurance authentication. In addition, there is an increasing need for improved physical security at federally owned and leased facilities and sites. Requirements are being identified to support electronic business at all levels of assurance with Federal business partners and agencies, which are experiencing a growing need to exchange information securely across network boundaries.

Agencies are working to address these challenges – PIV cards are being issued in increasing numbers, the Federal PKI has connected agency and commercial PKIs via a trust framework and working groups are tackling relevant questions in agency-and mission-specific situations. The CIO Council established the Identity, Credential, and Access Management Subcommittee (ICAMSC) with the charter to foster effective ICAM policies and enable trust across organizational, operational, physical, and network boundaries. The intersection of digital identities, credentials, and access control into one comprehensive management approach is made official along with the formalization of their interdependence.

The document, *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, was first published in November 2009, by the Federal CIO Council and an updated version (2.0) was published in December 2, 2011. The guidance document was developed in support of the ICAM mission to provide a common segment architecture and implementation guidance. The President's FY2010 budget did mention the development of the Federal ICAM segment architecture, stating that, "one of the major outcomes of this effort is to allow agencies to create and maintain information systems that deliver more convenience, appropriate security, and privacy protection, with less effort and at a lower cost."

The purpose of the ICAM guidance document is to provide agencies with architecture and implementation guidance that addresses existing ICAM concerns and issues they face daily. In addition to helping agencies meet current gaps, agencies stand to gain significant benefits around security, cost, and interoperability which will have positive impacts beyond an individual agency in improving the delivery of services by the Federal Government. It also seeks to support the enablement of systems, policies, and processes to facilitate business between the Government and its business partners and constituents. Benefits associated with implementation of ICAM include: increased security, compliance, improved interoperability, enhanced customer service, elimination of redundancy, increase in protection of personally identifiable information (PII).

These benefits promote standardized controls around identity and access management. The ICAM target state closes security gaps in the areas of user identification and authentication, encryption of sensitive data, and logging and auditing. It supports the integration of physical access control with enterprise identity and access systems, and enables information sharing across systems and agencies with common access controls and policies. The document is a call to action for ICAM policy makers and program implementers across the Federal Government to take ownership of their role in the overall success of the federal cyber security, physical security, and electronic government (E-Government) visions, as supported by ICAM. The roadmap document outlines several new agency initiatives and

[112] Sources: "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance," Federal CIO Council, version 2.0 December 2, 2011; Smart Card Alliance summary of the FICAM roadmap

[113] http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

[114] http://www.whitehouse.gov/open/

numerous supporting activities that agencies must complete in order to align with the government-wide ICAM framework, and critical to steps to address threats and challenges facing the Federal Government.

14.1 Overview of Identity, Credential and Access Management

This section provides an introduction to identity, credential, and access management (ICAM) referencing the primary compliance drivers: electronic authentication (E-Authentication) policy framework and two of its enablers, namely the HSPD-12 and Federal PKI initiatives. All ICAM programs within the Federal Government will align with the government-wide framework and interoperate with the infrastructure that supports it.

14.1.1 ICAM in the Federal Government

ICAM comprises the programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), and to bind those identities to credentials. ICAM cuts across numerous offices, programs, and systems within an agency's enterprise, which are typically directed and managed separately. Figure 11 provides a high-level overview of the complementary nature of different parts of ICAM and how concepts that were once viewed as stovepipes can intersect to provide an enterprise capability.

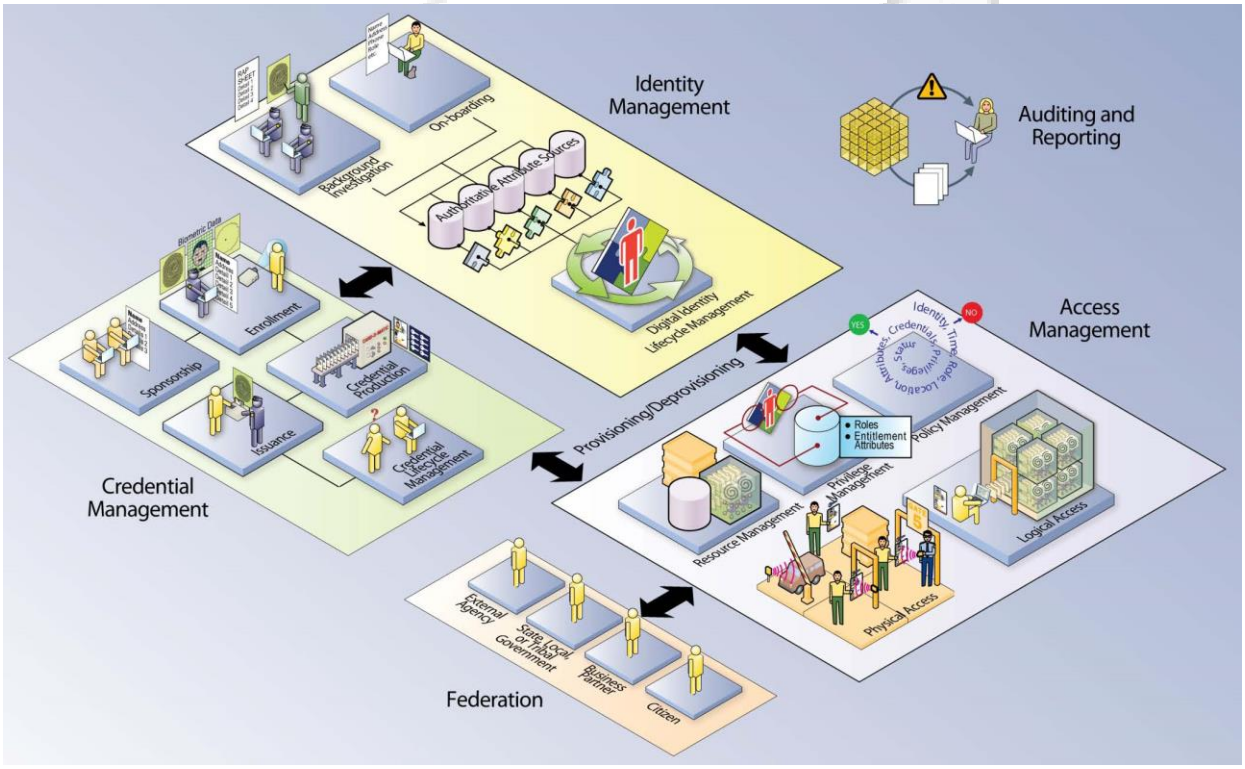


Figure 11. ICAM Conceptual Diagram

The following subsections provide additional detail on the constituent parts of ICAM and discuss the elements shown in Figure 11 in greater detail.

14.1.2 Identity Management

Identity management is defined as "the combination of technical systems, rules, and procedures that define the ownership, utilization, and safeguarding of personal identity information." The primary goal of identity management is to establish a trustworthy process for assigning attributes to a digital identity and

to connect that identity to an individual. The Federal ICAM document offers an approach to identity management wherein creation and management of digital identity records are shifted from stove-piped applications to an authoritative enterprise view of identity that enables application or mission-specific uses without creating redundant, distributed sources that are harder to protect and keep current. With the establishment of an enterprise identity, it is important that policies and processes are developed to manage the lifecycle of each identity where management includes a number of factors including schema framework, policies and procedures and protection of personally identifiable information (PII).

With the establishment of an enterprise identity, it is important that policies and processes are developed to manage the life cycle of each identity. Management of an identity includes:

- The framework and schema for establishing a unique digital identity,
- The ways in which identity data will be used,
- The protection of PII,
- Controlling access to identity data,
- The policies and processes for management of identity data,
- Developing a process for remediation; solving issues or defects,
- The capability to share authoritative identity data with applications that leverage it,
- The revocation of an enterprise identity, and
- The system that provides the services and capabilities to manage identity.

As part of the framework for establishing a digital identity, proper diligence should be employed to limit data stored in each system to the minimum set of attributes required to define the unique digital identity and still meet the requirements of integrated systems. A balance is needed between information stored in systems, information made available to internal and external systems, and the privacy of individuals.

14.1.3 Credential Management

According to NIST SP 800-63, a credential is, “an object that authoritatively binds an identity (and optionally, additional attributes) to a token possessed and controlled by a person.” Credential management supports the lifecycle of the credential itself. The policies around credential management, from identity proofing to issuance to revocation, are fairly mature compared to the other parts of ICAM. The PIV standards (e.g., FIPS 201, SP 800-73) and Federal PKI Common Policy are examples of documents which have been in place and are foundational to agency-specific credential implementations. Credentialing generally involves five major components:

1. Sponsorship,
2. Enrollment,
3. Credential production,
4. Issuance and
5. Credential management (maintained over its lifecycle), which might include:
    a. Revocation,
    b. Reissuance or replacement,
    c. Re-enrollment,
    d. Expiration,
    e. PIN reset,
    f. Suspension, or
    g. Re-instatement.

14.1.4 Access Management

Access management is the management and control of the ways in which entities are granted access to resources. The purpose of access management is to ensure that the proper identity verification is made when an individual attempts to access security sensitive buildings, computer systems, or data. It has two areas of operations: logical and physical access. Logical access is the access to an IT network, system, service, or application. Physical access is the access to a physical location such as a building, parking lot, garage, or office. Access management leverages identities, credentials, and privileges to determine access to resources by authenticating credentials and users of these credentials. After authentication (identity verification), a decision as to whether an individual is authorized to access the resource can be made (privilege verification). These processes allow agencies to obtain a level of assurance in the identity of the individual asking for access.

Three core support areas enable successful access management for both physical and logical access:

1. **Resource management** processes for establishing and maintaining data,
2. **Privilege management** processes for establishing and maintaining the entitlement or privilege attributes that comprise an individual's access profile; and
3. **Policy management** processes for establishing and maintaining policies that incorporate business rules and logic, usually based on attributes or roles. This governs what is allowable or unallowable in an access transaction.

14.1.5 ICAM Intersection

Understanding that ICAM programs have many areas of overlap is crucial to the overall success of these programs. There are many common elements associated with each of the areas addressed in the previous sections, including physical and logical access components, digital identities and attributes along with the systems that store them, and the workflow solutions that enable strong and dynamic processes. In fact, one of the primary dependencies across both the credentialing and the access control environments is the presence of accurate identity and attribute information necessary to bind the digital representation of an entity to a credential, user accounts, and access privileges. (While access can be granted based on provisioned identifiers, roles, other attributes or policy based decisions based on several contextual data points, the access decision must correspond to the correct digital identity.) As the necessity to complete transactions across networks with higher levels of assurance increases, so too does the need for the identity to be tied strongly and simultaneously to its high assurance credential, authoritative attributes, and access privileges. These overlaps demonstrate the intersection of identity, credential, and access management.

Challenges, nevertheless, exist to the adoption of a consistent approach to ICAM implementation. Addressing these challenges begins with viewing ICAM holistically. ICAM promotes a comprehensive, coordinated approach to help resolve the significant IT, security, and privacy challenges facing the Federal government. Just as identity, credential, and access management activities are not always self-contained and must be treated as a cross-disciplinary effort, ICAM also intersects with many other IT, security, and information sharing endeavors. It is expected that ICAM will touch many initiatives not specifically mentioned in the architecture and will be incorporated into holistic agency plans for their enterprise IT, mission and business service architectural segments.

14.2 ICAM Governance

The Federal ICAM Initiative is governed under the auspices of the Federal Chief Information Officer (CIO) Council, Identity Credential and Access Management Subcommittee (ICAMSC) with program support by the GSA Office of Government wide Policy (OGP), and direct oversight from the OMB. ICAMSC also works with other federal groups that have a broader focus on the national approach for identity management, whereas the ICAMSC is focused on identity management implementation efforts within the Federal government. In addition, stakeholders such as the Department of Commerce via the NIST and

the Office of Personnel Management (OPM) have oversight and responsibility for policy and standards for ICAM functions across the Executive Branch. Due to the large degree of overlap between the work of these groups, the ICAMSC is in close collaboration with the relevant stakeholders to help ensure consistency between the related efforts.

14.3 ICAM Segment Architecture

The ICAM segment architecture was developed under the auspices of the Federal CIO Council by a team of cross-agency representatives supporting the ICAMSC. The development team followed the approach outlined in the Federal Segment Architecture Methodology (FSAM) to create the ICAM segment.

The FSAM is a five-step process to help architects identify and validate the business need and scope of the architecture, define the performance improvement opportunities within the segment, and define the target business, data, services, and technology architecture layers required to achieve the performance improvement opportunities. The FSAM drives the creation of as-is state and future state descriptions, analysis of the gaps, and a transition plan for moving from the as-is to the future state over a specified period of time. A key objective of the ICAM segment architecture is to implement a holistic approach for all government-wide identity, credential, and access management initiatives and areas (including civilian, defense, health, financial, intelligence), which have traditionally been viewed and implemented separately.

Within each of the five process steps, the FSAM specifies a list of outputs associated with performing the high-level activities and provides sample templates. The FSAM was developed as a prescriptive methodology but was also designed to be flexible and extensible to allow for organization and segment specific adaptations. Since a segment architecture is typically created at the agency level, many of the outputs of the FSAM had to be tailored in order to successfully define a high-level architecture for ICAM at the federal (government-wide) level[115].

[115] See Figure 2 on page 26 of the "FICAM_Roadmap_and_Implementation_Guidance_v2 0_20111202_0.pdf" document which lists the segment architecture deliverables mapped to the document chapters.

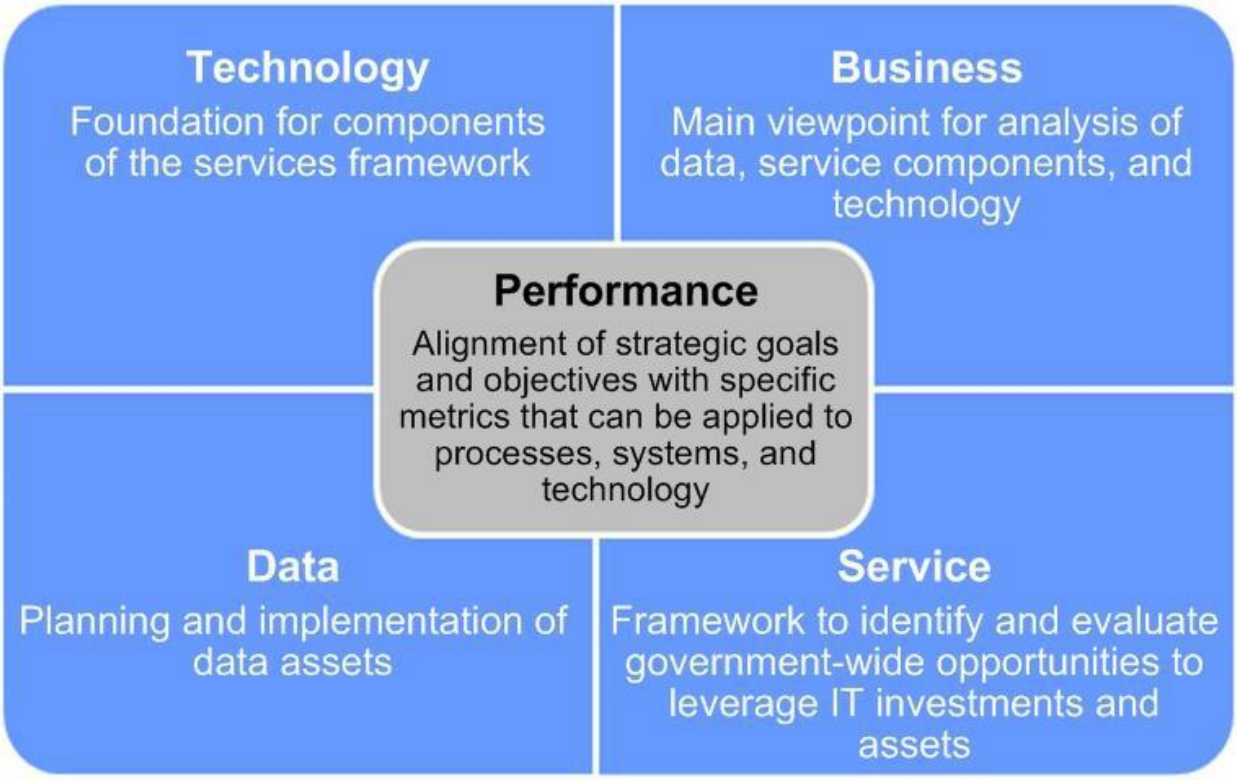


Figure 12. Segment Architecture Layers

14.3.1 Performance Architecture

The performance architecture aims to align strategic goals and objectives with specific metrics that can be applied to processes, systems, and technology in order to evaluate success against those goals. The goal of performance architecture is to provide the ability to take corrective action on performance results, the capability to measure resource contributions to specific mission value, and the ability to influence strategic objectives. Improved performance is realized through greater focus on mission, agreement on goals and objectives, and timely reporting of results.

The ICAM performance architecture consists of the following components:

- **Business Challenges Analysis**. Provides an overview of the challenges within the current ICAM environment. Business challenges often represent strategic improvement opportunities for the target state architecture.
- **Business Drivers, Goals, and Objectives**. Describes the goals, drivers, and objectives for ICAM.
- **Performance Metrics.** Create a reporting framework to measure the activities and investments within the ICAM segment.

Although the performance architecture is typically listed first among the segment layers, it frequently "book ends" the architectural development process, with the definition of strategic goals and objectives occurring in the earliest stages and the refinement and acceptance of performance metrics occurring as one of the last steps in creating the transition plan. The placement of the components of the performance architecture in the Roadmap reflects this split development of the layer.

14.3.2 Business Architecture

The business architecture is a functional perspective of the operations conducted within the ICAM segment. Segment architecture is driven by business management and delivers products that improve the delivery of business services to citizens and agency staff. As such, the business architecture provides the main viewpoint for the analysis of data, service components, and technology at the lower layers of the architecture.

The ICAM business architecture consists of the following components:

- **Business Value Chain Analysis**. Identifies the high-level logical ordering of the chain of processes that deliver value to one or more of the eGovernment sectors: government to citizen (G2C); government to business (G2B); government to government (G2G); internal efficiency and effectiveness (IEE).
- **As-is and Target Use Cases**. Provide the high-level common business processes that support ICAM functionality. The use cases provide the structure for the detailed architectural information at the data, service, and technology layers of the architecture. The guidance document identifies common use cases that capture the core ICAM business processes. The use cases are not agency specific and instead are intended to capture the common set of activities and challenges facing agencies today in the current state and the ways in which those challenges can be addressed in a desired target state. Agencies are expected to tailor these use cases for their own ICAM segment architectures, which should align with this document. Figure 13 summarizes the use cases defined in the guidance document.

Figure 13. ICAM Use Cases Overview

No.	Use Case Name	IEE	G2G	G2B	G2C	Use Case Description
1	Create and maintain digital identity record for internal user	√				Provides the high-level process steps for establishing a digital identity for an internal user and modifying the digital identity record overtime as the user's attributes change.
2	Create and maintain digital identity record for external user	√	√	√	√	Provides the high-level process steps for establishing a digital identity for an external user and modifying the digital identity record overtime as the user's attributes change.
3	Perform background investigation for federal applicant	√				Provides the high-level process steps for conducting a background investigation for a federal employee or contractor.
4	Create, issue, and maintain PIV card	√				Provides the high-level process steps for creating and issuing a PIV credential to a federal employee or contractor and maintaining it over the credential lifecycle in compliance with FIPS 201.
5	Create, issue, and maintain PKI credential	√	√	√	√	Provides the high-level process steps for creating, issuing, and maintaining a PKI certificate over the credential lifecycle in compliance with Federal PKI standards.
6	Create, issue, and maintain password token	√	√	√	√	Provides the high-level process steps for creating, issuing, and maintaining a password token over the credential lifecycle.
7	Provision and deprovision user account for an application	√	√	√	√	Provides the high-level process steps for provisioning and deprovisioning a user account and establishing the access privileges and entitlements for the user in an agency application.

No.	Use Case Name	IEE	G2G	G2B	G2C	Use Case Description
8	Grant physical access to employee or contractor	√				Provides the high-level process steps for authenticating and authorizing or denying a federal employee or contractor physical access to a facility or site.
9	Grant visitor or local access to federally-controlled facility or site	√	√	√	√	Provides the high-level process steps for authenticating and authorizing or denying a visitor (external to Federal government or individual from another agency) for physical access to federally-controlled facilities and sites.
10	Grant logical access	√	√	√	√	Provides the high-level process steps for authenticating and authorizing or denying a user logical access to systems, applications, and data. The use case provides alternate process flows to address authentication mechanisms at all four levels of assurance.
11	Secure document or communication with PKI	√	√	√	√	Provides the high-level process steps for digitally signing and encrypting data and electronic communications using the most common system tools available within the Federal government.

14.3.3 Data Architecture

Data architecture is the planning and implementation of data assets including the set of data, the processes that use that data, and the technologies selected for the creation and operation of information systems. From an enterprise architecture perspective, data architecture is not the set of detailed models of individual systems; instead, it provides the "big picture," including the information/data stored across the enterprise, the information that needs to be shared, and the ways in which that information should be shared through the use of exchange standards.

The ICAM data architecture consists of the following components:

- **Inventory of Government-wide Data Sources and Data Elements**. Lists and describes the major cross-government ICAM data repositories, the information contained in them, and the E-Government sectors they service.
- **Target Information Flow Diagrams**. Depicts the key information flows found in the business processes and assists in discovery of opportunities for re-use of information in the form of information-sharing services.

14.3.4 Service Architecture

The service architecture provides a functional framework for identifying and evaluating government-wide opportunities to leverage IT investments and assets from a service perspective. This model helps understand the services delivered by the government and assess whether there is an opportunity to group like services and create opportunities for reuse or shared services. The ICAM service architecture consists of the Services Framework, a functional framework that classifies ICAM service components with respect to how they support business and/or performance objectives.

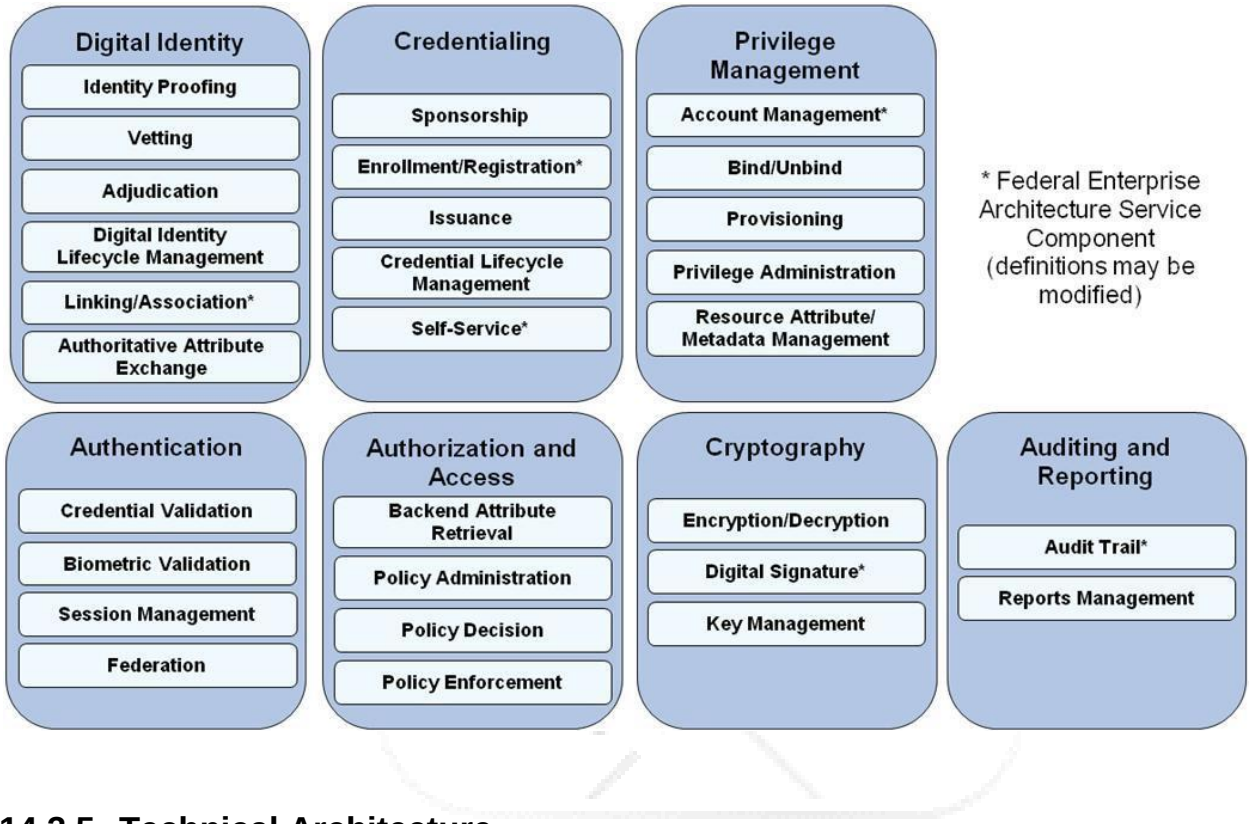
In order to develop the ICAM Services Framework, existing service frameworks from a number of sources were reviewed, including:

- FEA Service Component Reference Model (SRM)
- HSPD-12 Shared Component Architecture v0.1.6

- ISO/IEC JTC 1/SC27 N7237 - IT Security Techniques
- OneVA Identity Services Segment Architecture
- DoD Net-Centric Enterprise Services (NCES)
- DoD Enterprise Services Security Framework (ESSF)

Following the review, several working sessions were conducted to define and gain consensus on the service types and components necessary to support the ICAM segment. Figure 14 shows the resulting ICAM Services Framework.

Figure 14. ICAM Services Framework



14.3.5 Technical Architecture

The technical architecture provides the foundation for the components of the Services Framework, which in turn support the business layer and business-driven approach of the use cases. Specifically, the technical architecture is used to describe proposed technical solutions using a standard vocabulary and categorization scheme. As agencies propose solutions to fulfill the ICAM segment, the technical architecture allows those solutions to be analyzed for their fit with the desired target state, for duplication with other efforts, and for the architectural gaps they might fill. In addition, it facilitates the re-use of technology across agencies.

The ICAM technical architecture consists of the following components:

- **As-is System Interface Diagrams**. Provide a depiction of the as-is "conceptual solution architecture," which shows the existing systems and services in the as-is state and identifies the relationships between them.

- **Target System Interface Diagrams**. Provide a depiction of the target "conceptual solution architecture," which shows the proposed systems and services in the target state and identifies the relationships between them.

Additionally, the architecture analysis sections of each of the use cases provided in the guidance document include specific types of hardware and software and the technical standards at the ICAM data architecture layer to support the use case. Technical standards provide the types of product specifications needed, network protocols, or other technical components of the architecture.

In order to maintain government-wide applicability, the ICAM technical architecture is provided at a higher level than would typically be expected for a segment. As each agency aligns with the ICAM segment, the technical architecture may be translated to a more detailed level as needed by an agency to map the specific products and standards supporting ICAM systems to the overarching framework.

14.4 Summary

The FICAM Roadmap and Implementation Guidance is intended as a resource for agency implementers of identity, credential, and access management programs.

The Roadmap addresses unclassified federal identity, credential, and access management programs and how the Executive Branch of the Federal government will interact with external organizations and individuals. The scope of the guidance has been limited to ICAM programs that apply within and across the agencies in a variety of environments and configurations. This includes those associated with emerging IT advancements such as cloud computing, identity-as-a-service, and software-as-a-service. Using PIV certificates provides several benefits (strong authentication, standardized processes, digital signatures) and approved credentials must be supported by all applicable Federally procured services. It is anticipated that tailoring ICAM functionality to meet the unique mission requirements for particular programs that do not include access to federal IT systems or facilities will require additional collaboration and work outside the scope of the guidance document and the common ICAM initiative within the Federal government.

The document addresses the intersection of the Federal government with external entities from the perspective of the Federal government as a relying party of ICAM services and, to some extent, as an issuer of credentials. While detailed information is not provided about how an external entity should implement its own ICAM programs, the document provides information that is applicable to conducting business with the government where appropriate.

15 Other U.S. Government Smart Card Implementations[116]

This section profiles several U.S. government smart card implementations that either started before the FIPS 201 PIV Card program and are transitioning to FIPS 201 or are implementing PIV interoperable or compatible programs.

CSCIP Module 5, "Smart Card Usage Models – Identity and Security" includes additional profiles of the following government-related smart card applications: ePassport (Module 5, Section 4) and smart health cards (Module 5, Section 8.3).

15.1 Department of Defense Common Access Card

The Department of Defense (DoD) Common Access Card (CAC) was the first enterprise smart card program in the Federal Government. The DoD began deploying the CAC in 2000, and since then the CAC has been a single unifying card for the entire department with a growing number of applications.

The goal of the CAC program was to provide individuals with physical access to buildings and controlled spaces and logical access to networks and systems. These individuals are members of the active duty military personnel, civilian employees, and eligible contractor personnel. In addition to the original goals of physical and logical access the CAC is also used for benefits and privileges as well as being the Geneva Conventions card for United States.

This diverse range of uses and applications requires advanced card features. The CAC uses a 64-144K smart card platform, providing the flexibility to accommodate emerging space requirements and provide a solution for a growing range of technologies. The CAC includes four PKI certificates: identity certificate, email signing certificate, email encryption certificate and PIV authentication certificate. In order to be interoperable, the CAC card includes a PIV Card Application which, when selected, behaves as would any other government issued PIV Card. The card also includes basic demographic data, fingerprint biometrics and facial image, and contactless technology.

The CAC program has been successful for many reasons. The CAC is integral to DoD business practices which means cardholders are routinely using the card. Any changes to the card must be approved by the user community through a robust configuration management program. Also, the card is supported by policies and governance that clearly outline the uses and limitations of the card.

In compliance with Homeland Security Presidential Directive 12/HSPD-12, the DoD began issuing its FIPS 201-compliant CAC in October 2006. Because of the maturity of the CAC program, a significant transition strategy was required to ensure continuity of operations. The CAC now fully complies with PIV standards and provides interoperability when used in other Federal Agencies, but the primary functionality of the card remains DoD focused.

The CAC is currently being considered for additional functions and applications. Some potential new areas of use are transportation and banking. Some applications could use the card as a payment system for transit systems and use the card instead of a bank card in some instances.

15.1.1 DoD Identity Management

The DoD has unique challenges that must be solved through its personnel identity management solutions. In addition to those individuals that receive CACs[117], the DoD population includes millions of dependents and retirees and other individuals that require routine access to DoD facilities and assets[118]. DoD is working to align the needs of the populations with the current solutions and to `provide additional services where necessary.

[116] These profiles are also included in CSCIP *Module 5, Smart Card Usage Models – Identity and Security,* Section 8.

[117] DoD has about 3.14 million employees and 0.5 million contractors, all CAC/PIV cardholders. It is the largest PIV deployment.

[118] The Department of Veterans Affair (VA) is the second largest PIV deployment in the Federal government with more than 420 thousand PIV Cards in use.

To serve these populations, the DoD has a number of identity management solutions including: the family of DoD ID cards, the Defense Biometrics Identification System (DBIDS), the Defense National Visitors Center (DNVC), and the Defense Cross-Credentialing Identification System (DCCIS).

DBIDS is a readily deployable system for capturing, storing, and comparing biometric data to use for authentication. The system also provides a means of registering all personnel requiring access, incorporating complex rules of sponsorship and access, linking access to sponsor, and limiting access by location, building, and force protection level. In addition, DBIDS allows installation security personnel to control access and authenticate identity for population elements not eligible for other DoD credentials, including maintenance personnel, janitorial staff, and contractor personnel from non-DoD organizations.

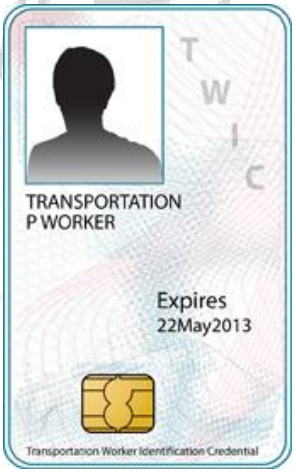
The ability to rapidly electronically authenticate credentials and cardholders is critical to being able to operate in a federated environment. DNVC is the system that can electronically validate any centrally issued DoD credential. DNVC can accommodate different readable formats and provides a real-time determination of validity in a privacy-friendly manner. The DNVC is web-based and provides a means for strengthening security across the DoD down to the lowest levels.

DCCIS is an extension of DNVC. DCCIS is an initial proof-of-concept system that proposes to resolve cross-credentialing interoperability difficulties between DoD and certain of its commercial partners. DNVC can be DCCIS-enabled, in which case a participating DNVC facility connects with the DCCIS member organization database to authenticate visiting personnel from those organizations.

Not all needs are being met by current capabilities. Access to online applications for non-CAC populations has been difficult and is under consideration. A potential solution to meet this need may include federated electronic credentials for these populations. DoD is also working to align its capabilities with the requirements of the Federal Identity, Credentialing and Access Management Sub-Committee. As such, DoD will continue to evolve and transform to meet the changing needs.

15.2 Transportation Worker Identification Credential[119]

The Transportation Worker Identification Credential (TWIC) program is a joint program of the Transportation Security Administration (TSA) and the U.S. Coast Guard (USCG) within the Department of Homeland Security (DHS). The objective of TWIC is to strengthen the security of the U. S. maritime infrastructure through background vetting of civilian maritime workers and issuance of tamper-resistant biometrically-enabled identification credentials to eligible workers. TWIC was developed in response to the legislative requirements contained in the Maritime Transportation Security Act (MTSA) of 2002 (Public Law 107-295) and the Security and Accountability for Every Port (SAFE Port) Act of 2006 (PL 109-347).



As of April 2015, over 3 million maritime workers have enrolled in the TWIC program. Possession of a TWIC card since April 2009 is required for unescorted access at 3,200 land-based and outer continental shelf (OCS) facilities and on over 14,000 vessels that are subject to MTSA regulations. Workers pay for the TWIC which is $128.00 for a five-year card as of February 2015.

TWIC is aligned with FIPS 201 and includes the following technical features:[120]

- 64K of non-volatile memory
- Dual-interface smart card chip with both contact and contactless interfaces

[119] Source: "Authentication Mechanisms for Physical Access Control," Smart Card Alliance Physical Access Council white paper, October 2009

[120] "Transportation Worker Identification Credential: An Overview of TWIC Reader Hardware and Card Application Specification," Walter Hamilton, IBIA, presentation, Smart Cards in Government Conference, October 2008

- Physical security features, color shifting inks
- Magnetic stripe and linear bar code
- Logical security features, including: encrypted fingerprint templates, signed data (CHUID and biometrics), security objects, and PKI certificates (for the PIV application).

In the early stages of defining the technical requirements for the TWIC card, the maritime industry expressed concerns about the proposed approach, which called for the TWIC card to be fully compliant with the FIPS 201 standard. The maritime community felt that FIPS 201 was not an appropriate standard for high volume physical access control situations in which rapid access is an operational imperative. Their concerns were based on the fact that FIPS 201 allows access to the biometric data on the smart card only through a contact interface, thereby requiring insertion of the card into a contact interface slot on a reader. Given that many of the fixed mounted reader devices would be exposed to the extremes of weather at seaports, there was concern that contact readers would allow airborne contaminants to infiltrate the reader electronics, resulting in frequent maintenance problems. The maritime industry also objected to the FIPS 201 requirement for entry of a PIN to access the biometric data on the smart card after insertion of the card into the reader.

The resulting "TWIC Reader Hardware and Card Application Specification," initially published by TSA on September 11, 2007, implements an alternative authentication mechanism that allows contactless reading of the reference fingerprint template from a separate TWIC card application without requiring PIN entry. The TWIC card supports a GSA approved PIV Card application in addition to this specialized TWIC card application. To protect personal privacy, the fingerprint templates stored on the TWIC card application are pre-enciphered by the issuer prior to being loaded to the TWIC card application. Deciphering of these TWIC card application fingerprint templates is accomplished through the use of a randomized, unique per card symmetric key called the TWIC Privacy Key (TPK). The TPK is generated during card personalization by TSA. The TPK can be accessed through the contact interface or through a swipe read of the magnetic stripe or from an off-card database supported by some TWIC reader implementations. The point is the TPK cannot be accessed using the contactless interface as such access would break the security against a third party observing a contactless transaction.

This approach to using a contactless biometric read without PIN presents some unique challenges for the implementer. If the pre-enciphered biometric templates are to be read from the TWIC card application through the contactless interface, the reader must have some way of first obtaining the TPK prior to performing the biometric match. This can be achieved by storing the TPK in the local PACS server after a one-time local PACS registration process. Another alternative is to use a reader that has both magnetic stripe and contactless smart card read capability. In this scenario, the cardholder would swipe the magnetic stripe of TWIC card before presenting the card to the contactless interface. Finally, one might use a contact interface where the enciphered fingerprint templates and the TPK are accessible.

As noted above, a TWIC card consists of two card applications: a TWIC card application to support contactless, PIN-less biometric reads independent of smart card interface, and a separate FIPS 201-compliant PIV Card application, each of which are co-located in the memory of a TWIC card. A reader device can access each application independently by selecting the appropriate application identifier (AID).

Table 15 shows a summary of the primary differences between the TWIC and PIV credentials.

Table 15. Differences between TWIC and PIV *Credentials*[121]

Category	PIV Card application	TWIC card application
Stored fingerprint templates	Data not encrypted. Requires PIN to read via contact or contactless interface.	Data encrypted. No PIN required to read via contact or contactless interface.
TWIC Privacy Key (TPK)	Not applicable	Stored in magnetic stripe. Also accessible through contact interface. Required to decrypt stored fingerprint templates.

In late 2012, Congress passed legislation requiring TWIC to implement an issuance solution requiring only one visit to an enrollment center. This option is referred to as the OneVisit option. The OneVisit option presented significant FIPS 201 challenges to the TWIC program as the applicant has the TWIC card mailed to a location they designate. Direct mailing removes the possibility of in-person card activation (after a biometric match or alternative identification verification step). It is estimated 7 out of 10 TWIC applicants select the OneVisit option.

Current regulations do not require the use of TWIC readers that automatically read the TWIC card, match the biometric to the cardholder, and validate other electronic security features in the card. As of April 2009, only visual inspection of TWIC cards is required for unescorted entry into regulated facilities and vessels. TSA conducted an extensive field pilot test from August 2008 until May 2011. The test of TWIC readers was to measure their effectiveness and impact on operations. The field pilot data analysis was used to inform the next phase of rulemaking which will establish U.S. Coast Guard regulations governing the use of TWIC readers. Under this new rule making, it is expected that the requirement for use of TWIC readers will be based on a risk management approach that will strike a balance between criticality to the nation's infrastructure, the consequence of a transportation incident, and the utility of the TWIC reader in an operational environment.

15.3 First Responder Authentication Credential[122]

The First Responder Authentication Credential (FRAC) is an excellent example of the use of a PIV-interoperable credential.

In the wake of 9/11 and Hurricane Katrina, U.S. homeland security professionals learned that responding to a disaster requires a multi-disciplinary response team including law enforcement, firefighters, medical professionals, and critical infrastructure workers. These emergency responders represent a broad array of disciplines within the local and state emergency management organizations and it is crucial for the incident command to recognize, in real-time, the certifications and abilities of each individual responding to the incident.

The Office of National Capital Region Coordination coordinated a major initiative to leverage a smart card identity system (the First Responder Authentication Credential) for emergency response officials (EROs). These smart cards would provide first responders from across with the region the ability to quickly and easily access government buildings and reservations in the event of a terrorist attack or other disaster. The initiative was designed to remedy access problems such as those encountered by state and local emergency officials responding to the 9/11 attack on the Pentagon.

[121] It must be understood the TWIC card contains two different card applications: one which is compliant with the PIV technical specifications and another card application which contains the TWIC required data structures. So the TWIC credential is a card with two applications either of which can be selected depending on the mode the terminal wants to work with.

[122] Sources: DHS web site, http://www.dhs.gov/xfrstresp/standards/editorial_0849.shtm; Probaris: "First Responder Authentication Credentials" white paper.

FRAC is a secure and interoperable identity credential designed for the emergency management community. NIST, DHS and the Federal Emergency Management Agency (FEMA) have worked together to specify the recommendations for the FRAC card for all emergency responders nationwide. Adherence to these recommendations ensures a common framework to trust the identities and capabilities of those emergency response team members arriving at incidents to assist during emergencies. By leveraging the US Government FIPS-201 Personal Identity Verification standard, and the accompanying PIV-interoperable guidance from the CIO Council[123], interoperable identity verification is achieved among federal, state, local, non-profit and commercial organizations responding to an incident.

Under DHS National Incident Management System (NIMS) draft credentialing guidelines, three distinct and necessary components are required for an emergency responder credential:

- **Identity:** personal attributes that uniquely define a person
- **Knowledge, skills and attributes (KSAs):** certifications, trainings and NIMS resource typing that allow an incident commander to make access and deployment decisions
- **Deployment authorizations:** the invitation from a requesting jurisdiction, and authorization from the supporting jurisdiction, for an emergency response individual or team to respond to a mutual aid incident. Deployment authorizations are widely used in multi-jurisdictional responses crossing state boundaries. Deployment authorizations typically follow Emergency Management Assistance Compacts (EMAC) processes.

At an incident scene, it is imperative to accurately verify both a person's identity and KSAs . In locales around the country, there are regular news and online stories of individuals pretending to be a police officer or a firefighter or an emergency medical technician. Official-looking badges and clothing are available for purchase via catalogs and websites and, during the high intensity of a disaster, these fraudulent items can fool even the most experienced veteran responders. Unfortunately there are also cases where valid emergency responders are detained or delayed because they do not have an easy way to establish identity or KSAs at a checkpoint.

A person's identity can only be trusted if it's confirmed, issued and verifiable via a trusted issuing source. The NIMS has published the resource typing categories and certifications for Emergency Support Functions (ESFs) and National Infrastructure Protection Plan (NIPP). States and jurisdictions are required to identify and maintain lists of individuals who have the correct training and certifications for each of these NIMS categories. Privileges granted at an incident depend upon knowing the emergency responder's ESF codes or NIPP sectors, training, certifications and licensure information.

15.3.1 PIV-I/FRAC Technology Transition Working Group[124]

Local and state emergency response officials must be able to collaborate to ensure the public's safety. However, for this to happen, many identity management challenges must be overcome. While federal agencies are rapidly deploying secure common identification standards based on guidance from the White House and other federal entities, state and local emergency response officials are working to establish a Personal Identity Verification-Interoperable (PIV-I) / First Responder Authentication Credential (FRAC) standard that is interoperable between local, state, and federal levels.

The Cyber Security Division (CSD) within the Science and Technology Directorate (S&T), the FEMA Office of National Capital Region Coordination (NCRC), the FEMA Office of the Chief Security Officer (OCSO), and the FEMA Office of the Chief Information Officer (OCIO) have partnered to convene the PIV-I/FRAC Technology Transition Working Group (TTWG).

The TTWG is composed of state and local emergency management representatives, many of whom have already implemented innovative and secure identity-management solutions in their own jurisdictions.

---

[123] "Personal Identity Verification Interoperability for Non-Federal Issuers," CIO Council, July 2010, http://www.idmanagement.gov/sites/default/files/documents/PIV_IO_NonFed_Issuers.pdf

[124] http://www.dhs.gov/piv-ifrac-technology-transition-working-group

The purposes of the working group are to:

- Provide federal policy makers with a unified State emergency manager perspective on Federal/Emergency Response Official (F/ERO) attributes
- Baseline current identity infrastructure and best practices to share with stakeholders
- Identify technological gaps where CSD can provide test bed research and development support
- Share information: state-to-state, state-to-federal, federal-to-state.

Local and state participants as of August 1, 2013:

- Colorado
- Maryland
- Virginia
- District of Columbia
- Missouri
- Southwest Texas
- Pennsylvania
- Chester County, PA
- Pittsburgh, PA
- West Virginia
- Hawaii
- Rhode Island

15.3.2 Commonwealth of Virginia First Responder Authentication Credentials[125] [126]

EROs from across the region were present at the Pentagon site on 9/11, including EROs from Arlington County and the City of Alexandria. Immediately following the attacks, onlookers were able to mingle with rescuers. This presented a serious challenge for incident commanders—to make sure that only credentialed EROs had access to the most sensitive areas. It became evident that a credentialing process was needed to simplify this effort in the future.

In February 2007, as part of the DHS National Capitol Region (NCR) First Responder Partnership Initiative, the Virginia Department of Transportation and Commonwealth of Virginia began issuing FRACs. The Virginia FRAC identity proofing and registration processes follow FIPS 201 as closely as possible for a non-Federal entity and use products from the FIPS 201 GSA Approved Products List. The design of the Virginia FRAC card was also based upon FIPS 201.

The goal of the FRAC initiative, now being deployed in the NCR and Hampton Roads area, is to provide state and local EROs with a new, Federally-approved PIV-interoperable smart credential designed to achieve the following:

- Securely establish emergency responders' identities at the scene of an incident
- Confirm first responders' qualifications and expertise, allowing incident commanders to dispatch them quickly and appropriately
- Enhance cooperation and efficiency between state and local first responders and their federal counterparts

Using a wireless handheld device, commanders at an incident scene can read and validate data from the FRAC and authenticate the ERO's identity and attributes.

Among the first localities in Virginia to be issued the new FRACs were Arlington County and the City of Alexandria (initial deployment was for 2,300 FRACs in 2006). Virginia is now working on a FRAC deployment in the Hampton Roads region. This deployment includes eight locations for the biometric enrollment and issuance of PIV-interoperable credentials, 39 handhelds for offline credential validation and 12,900 FRACs.[127]

[125] "Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery," Smart Card Alliance white paper, October 2008, http://www.smartcardalliance.org/pages/publications-emergency-response-official-credentials

[126] http://dls.virginia.gov/commission/Materials/FRAC.pdf

[127] Source: "Commonwealth of Virginia First Responder Authentication Credential (FRAC) Program, W.Duane Stafford, Governor's Office of Veterans Affairs and Homeland Security, http://dls.virginia.gov/commission/Materials/FRAC.pdf

16 Standards, Policy Guidance and References

16.1 Standards

This section lists the NIST standards and special publications and other standards referenced in this module that are relevant to FIPS 201 and Federal identity management.

- ANSI INCITS 322 Information Technology, Card Durability Test Methods, ANSI, 2008
- ANSI INCITS 378, "Information technology - Finger Minutiae Format for Data Interchange," ANSI, 2009
- FIPS 140-2, Federal Information Processing Standard Publication 140-2 (FIPS 140-2), "Security Requirements for Cryptographic Modules," May 2001, http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
- FIPS 199, Federal Information Processing Standard 199 (FIPS 199), "Standards for Security Categorization of Federal Information and Information Systems," February 2004, http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf
- FIPS 201-2, Federal Information Processing Standard Publication 201 (FIPS 201), "Personal Identity Verification (PIV) of Federal Employees and Contractors," August 2013, http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf
- ISO/IEC 7810, Identification Cards – Physical Characteristics – Published in 2003. Two amendments published: Amd 1 in 2009 and Amd 2 in 2012.
- ISO/IEC 7816, Identification Cards – Integrated Circuit Cards 14 different parts, not all relevant to PIV. Publication dates of the PIV relevant parts latest versions varies between 2004 and 2014
- ISO/IEC 10373, Identification Cards – Test Methods. 9 different parts, not all relevant to PIV. Publications dates vary from 2006 to 2014.
- ISO/IEC 14443, Identification Cards – Contactless Integrated Circuit(s) Cards – Proximity Cards. 4 different parts. Publication dates vary from 2008 to 2014
- NIST Interagency Report 6887 (NISTIR 6887), "Government Smart Card Interoperability Specification," Version 2.1, July 2003, http://csrc.nist.gov/publications/PubsNISTIRs.html
- NIST Interagency Report 7123 (NISTIR 7123), "Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report," NIST, June 2004, http://csrc.nist.gov/publications/PubsNISTIRs.html
- NIST Interagency Report 7452, (NISTIR 7452), "Secure Biometric Match-on-Card Feasibility Report," November 2007,http://csrc.nist.gov/publications/PubsNISTIRs.html NIST Interagency Report 7477 (NISTIR 7477), "Performance of Fingerprint Match-on-Card Algorithms Phase II/III Report," May 21, 2009, http://csrc.nist.gov/publications/PubsNISTIRs.html
- NIST Special Publication 800-53 (SP 800-53 Revision 4), "Recommended Security Controls for Federal Information Systems," April 30,2013, http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf
- NIST Special Publication 800-57 (SP 800-57), "Recommendation for Key Management,"
    - Part 1- General - Revision 3 (July 2012) http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
    - Part 2: Best Practices for Key Management Organization (August 2005) . http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

- Part 3: Application-Specific Key Management Guidance – Revision 1 (January 2015) http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57Pt3r1.pdf

- NIST Special Publication 800-63 (SP 800-63-2), "Electronic Authentication Guideline," August 2013. http://csrc.nist.gov/publications/nistpubs/800-64-Rev2/SP800-64-Revision2.pdf
- NIST Special Publication 800-73-4 (SP 800-73-4 Draft), "Interfaces for Personal Identity Verification (4 Parts)," May 19,2014, http://csrc.nist.gov/publications/PubsSPs.htmlNIST Special Publication 800-76-2, "Biometric Data Specification for Personal Identity Verification," (SP 800-76-2), July 2013, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-78-3 (SP 800-78-3), "Cryptographic Algorithms and Key Sizes for Personal Identity Verification," (SP 800-78-3), December 2010, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-79-2 (Draft), "Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers (DPCI)", June 2, 2014, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-85 A-2 (SP 800-85 A-2)[128], "PIV Card Application and Middleware Test Guidelines," July 2010, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-85 B-4 (SP 800-85 B-4 Draft), "PIV Data Model Test Guidelines," August 6, 2014 http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-87 (SP 800-87-1), "Codes for Identification of Federal and Federally-Assisted Organizations," April 2008, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-96 (SP 800-96), "PIV Card to Reader Interoperability Guidelines", September 2006, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-116 (SP 800-116), "A Recommendation for the Use of PIV Credentials in Physical Access Control Systems (PACS)," November 2008, http://csrc.nist.gov/publications/PubsSPs.html
- NIST Special Publication 800-156, (SP 800-156), "Representation of PIV Chain-of-Trust for Import and Export", Publication announced in FISP 201-2 but not yet available on the NIST web site even as a draft.
- NIST Special Publication 800-157, "Guidelines for Derived Personal Identity Verification (PIV) Credentials", December 2014, http://csrc.nist.gov/publications/PubsSPs.html
- Personal Computer/Smart Card (PC/SC) Specification, http://www.pcscworkgroup.com/
- "PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1," published by the authority of the Secretary General, International Civil Aviation Organization, October 1, 2004, http://www.csca-si.gov.si/TR-PKI_mrtds_ICC_read-only_access_v1_1.pdf
- RFC 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol (OCSP)," Internet Engineering Task Force (IETF), http://www.ietf.org/rfc/rfc2560.txt
- RFC 4122, "A Universally Unique Identifier (UUID) URN Namespace," Internet Engineering Task Force, July 2005, http://www.ietf.org/rfc/rfc4122.txt
- "Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems" (TIG SCEPACS), Physical Access Interagency Interoperability Working Group, Government Smart Card Interagency Advisory Board, July 30, 2004, http://www.idmanagement.gov/sites/default/files/documents/TIG_SCEPACS_v2.2.pdf

[128] This version is not yet updated for FIPS 201-2 and refers only to SP 800-74-3 version.

16.2 Policy Documents

This section lists the U.S. policy mandates and guidance documents that have been issued that are relevant to FIPS 201 and Federal identity management and that were referenced in this module.

- "Acquisition of Products and Services for Implementation of HSPD-12," OMB Memorandum M06-18, June 30, 2006, http://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2006/m06-18.pdf
- "E-Authentication Guidance for Federal Agencies," OMB Memorandum M04-04, December 16, 2003, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy04/m04-04.pdf
- "Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services," OMB Memorandum M05-05, December 20, 2004, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-05.pdf
- Electronic Signatures in Global and National Commerce Act (the E-Sign Act), https://www.fdic.gov/regulations/compliance/manual/pdf/X-3.1.pdf or http://www.gpo.gov/fdsys/pkg/PLAW-106publ229/pdf/PLAW-106publ229.pdf
- "Federal Identity, Credential and Access Management (FICAM) Roadmap and Implementation Guidance," Version 2.0, Identity, Credential and Access Management Subcommittee (ICAMSC), Federal CIO Council, December 2, 2011, http://www.idmanagement.gov/sites/default/files/documents/FICAM_Roadmap_and_Implementation_Guidance_v2%200_20111202_0.pdf
- FICAM Testing Program Documents can be found at http://www.idmanagement.gov/ficam-testing-program-documents
- Government Paperwork Elimination Act, http://www.archives.gov/records-mgmt/policy/electronic-signature-technology.html and http://www.whitehouse.gov/omb/fedreg_gpea2/
- "Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors," OMB Memorandum M-05-24, August 5, 2005, http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2005/m05-24.pdf
- "Personal Identity Verification Interoperability for Non-Federal Issuers," CIO Council, July 2010, http://www.idmanagement.gov/sites/default/files/documents/PIV_IO_NonFed_Issuers.pdf
- "Policy for a Common Identification Standard for Federal Employees and Contractors," Homeland Security Presidential Directive 12 (HSPD-12), August 27, 2004, http://www.dhs.gov/homeland-security-presidential-directive-12
- "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002," Office of Management and Budget (OMB) Memorandum M-03-22, September 26, 2003, http://www.whitehouse.gov/omb/memoranda_m03-22/
- "Protection of Sensitive Agency Information," OMB Memorandum M06-06, June 23, 2006, http://www.whitehouse.gov/OMB/memoranda/fy2006/m06-16.pdf
- "Shared Service Provider Repository Service Requirements," Federal Public Key Infrastructure Policy Authority, December 13, 2011, http://www.idmanagement.gov/sites/default/files/documents/SSPrepositoryRqmts.doc
- "Streamlining Authentication and Identity Management within the Federal Government," OMB Memorandum, July 3, 2003, http://www.whitehouse.gov/sites/default/files/omb/inforeg/eauth.pdf
- "X.509 Certificate and CRL Extensions Profile for the SSP program," Version 1.8, Federal Public Key Infrastructure Policy Authority, January, 2008 http://www.idmanagement.gov/sites/default/files/documents/CertCRLprofileForCP.pdf

- "X.509 Certificate Policy for the E-Governance Certification Authorities," http://www.idmanagement.gov/sites/default/files/documents/EGovCA-CP.pdf
- "X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework," Federal Public Key Infrastructure Policy Authority, http://www.idmanagement.gov/sites/default/files/documents/CommonPolicy.pdf

16.3 Other References

This section lists other references used for this module.

- "Access America: Reengineering through Information Technology," report of the National Performance Review and the Government Information Technology Services Board and Vice President Al Gore, February 3, 1997. Available as a book or an e-book.
- "Authentication Mechanisms for Physical Access Control," Smart Card Alliance Physical Access Council white paper, October 2009
- HSPD-12 PUBLIC REPORT SUMMARY ("PIV Card Status"), http://www.whitehouse.gov/sites/default/files/omb/assets/egov_docs/hspd-12_reporting_workbook_q2fy2013_public_report.pdf
- "Cybersecurity Efforts within the DoD," Bob Gilson, Department of Defense/Defense Manpower Data Center, presentation, Smart Cards in Government Conference, October 2009
- "DoD Implementation of Homeland Security Presidential Directive-12," Inspector General, U.S. Department of Defense, Report No. D-2008-104, June 23, 2008, p. 38, http://www.dodig.mil/Audit/reports/fy08/08-104.pdf
- E-Government Act of 2002, http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf
- "Emergency Response Official Credentials: An Approach to Attain Trust in Credentials across Multiple Jurisdictions for Disaster Response and Recovery," Smart Card Alliance white paper, October 2008, http://www.smartcardalliance.org/pages/publications-emergency-response-official-credentials
- "The Evolving Federal Public Key Infrastructure," Federal Public Key Infrastructure Steering Committee, Federal CIO Council, June 2000, http://www.idmanagement.gov/documents/evolving-federal-public-key-infrastructure
- Federal Public Key Infrastructure Policy Authority, http://www.idmanagement.gov/federal-public-key-infrastructure
- FIPS 201 Evaluation Program, http://www.idmanagement.gov/ficam-testing-program
- GSA USAccess web site, http://www.gsa.gov/portal/category/27240
- "HSPD-12: Defining a Federal PKI Framework," Judith Spencer presentation, Smart Cards in Government Conference, April 2006
- "HSPD-12 Implementation Status Reports," OMB, http://www.whitehouse.gov/omb/e-gov/hspd12_reports/
- "Levels of Authentication Brief," Smart Card Alliance Identity Council brief, March 2010, http://www.smartcardalliance.org/pages/publications-assurance-levels-overview-and-recommendations
- The Comprehensive National Cybersecurity Initiative, http://www.whitehouse.gov/issues/foreign-policy/cybersecurity/national-initiative

- NIST Cryptographic Module Validation Program (CMVP), http://csrc.nist.gov/groups/STM/cmvp/index.html
- NIST National Voluntary Laboratory Accreditation Program (NVLAP), http://www.nist.gov/nvlap/
- NIST Personal Identity Verification Program (NVIVP), http://csrc.nist.gov/groups/SNS/piv/npivp/index.html
- The Open Government Initiative, http://www.whitehouse.gov/open/
- "Physical Access Control: An Overview of the Impact of FIPS 201 on Federal Physical Access Control Systems," Smart Card Alliance white paper, September 2005, http://www.smartcardalliance.org/pages/publications-fips-201-impact
- "Physical Access Control System Migration Options for Using FIPS 201-1 Compliant Credentials," Smart Card Alliance Physical Access Council white paper, September 2007, http://www.smartcardalliance.org/pages/publications-pacs-migration-options
- Privacy Act of 1974, http://www.justice.gov/opcl/privacy-act-1974
- "The Realized Value of the Federal Public Key Infrastructure," Identity, Credential and Access Management Sub Committee (ICAMSC), January 29, 2010, http://www.idmanagement.gov/sites/default/files/documents/RealizedValueFederalPKI.pdf
- "Transportation Worker Identification Credential (TWIC)," John Schwartz, TSA, presentation, CTST 2008, May 2008
- "Transportation Worker Identification Credential: An Overview of TWIC Reader Hardware and Card Application Specification," Walter Hamilton, IBIA, presentation, Smart Cards in Government Conference, October 2008
- "TWIC Reader Hardware and Card Application Specification," TSA, Version 1.1.1 May 2012, http://www.tsa.gov/sites/default/files/publications/pdf/twic/twicreaderhardwareandcardapplicationspecification.pdf
- "Using FIPS 201 and the PIV Card for the Corporate Enterprise," Smart Card Alliance white paper, October 2008, http://www.smartcardalliance.org/pages/publications-piv-corporate-enterprise
- "Using PIV for Network Access," Anna Fernezian, ActivIdentity, presentation during *Using PIV for Physical and Logical Access Workshop* at Smart Cards in Government Conference, October, 2008
- "What Makes a Smart Card Secure?," Smart Card Alliance white paper, October 2008

17 Annexes

17.1 HSPD -12 Credentials in Use as of December 1, 2013

Agency Name	Acronym	Total Number of			Total Number of PIV cards required	Total Number of PIV cards issued	% achieved
		Employees	Contractors	Others			
		Requiring PIV credentials					
Department of Defense	DoD	3,137,577	501,888	-	3,639,465	**3,638,867**	99.98%
Department of Veterans Affairs	VA	343,954	25,772	71,563	441,289	**422,276**	95.69%
Department of Homeland Security	DHS	303,768	88,311	4,087	396,166	**396,166**	100.00%
Department of Health and Human Services	HHS	158,096	66,514	16,653	241,263	**118,260**	49.02%
Department of the Treasury	Treas	110,011	7,780	-	117,791	**110,281**	93.62%
Department of Agriculture	USDA	98,000	9,921	7,212	115,133	**89,742**	77.95%
Department of Justice	DOJ	80,652	18,923	9	99,584	**73,429**	73.74%
Social Security Administration	SSA	74,237	25,631	-	99,868	**99,868**	100.00%
Department of the Interior	DOI	64,013	8,205	3,054	75,272	**72,068**	95.74%
Department of Transportation	DOT	55,393	27,015	-	82,408	**80,143**	97.25%
Department of State	State	48,375	21,099	-	69,474	**69,474**	100.00%
Department of Commerce	DOC	44,519	10,213	622	55,354	**46,836**	84.61%
National Aeronautics and Space Administration	NASA	18,442	53,731	1,177	73,350	**68,529**	93.43%
Department of Labor	DOL	16,162	3,532	-	19,694	**15,739**	79.92%
Environmental Protection Agency	EPA	16,088	3,065	1,265	20,418	**20,025**	98.08%
Department of Energy	DOE	14,860	89,867	66	104,793	**88,408**	84.36%
General Services Administration	GSA	11,852	26,184	-	38,036	**30,431**	80.01%
All agencies with less than 10,000 cards each (71 Agencies)		67,997	26,803	287	95,087	**71,412**	75.10%
Totals		**4,663,996**	**1,014,454**	**105,995**	**5,784,445**	**5,511,954**	**95.29%**

17.2 Secure Messaging Fundamentals

Per ISO/IEC 7816 Part 4 "*The goal of secure messaging (SM) is to protect [part of] the messages to and from a card by ensuring two basic security functions: data integrity and data confidentiality.*

Secure messaging is achieved by applying one or more security mechanisms. Each security mechanism involves an algorithm, a key, an argument and often, initial data."

Secure messaging can provide:

A. Message integrity through computation of a Message Authentication Code (MAC).

B. Confidentiality by enciphering the command data (and often the response data as well) using a block cipher algorithm.

C. Transaction sequence obfuscation by using either the ENVELOPE command that encapsulates the entire command APDU (i.e. the Command Header and Command Data) into an enciphered message or use of secure messaging tag '89'.

Entity authentication is not specified as part of secure messaging but is typically required in some form by the scheme using secure messaging. It is interesting that some secure messaging implementations choose to only authenticate the card while others require both the card and terminal to be authenticated (to each other).

ISO/IEC 7816 does not mandate a particular key type, cryptographic algorithm, or mode of cryptographic algorithm. This permits flexibility in terms of industry need and practices. However the use of block ciphers is specified.

Specifically per Clause 6 of ISO/IEC 7816 Part 4 "*The computation of a cryptographic checksum involves an initial check block, a secret key and either a block cipher algorithm (see ISO/IEC 18033), or a hash-function (see ISO/IEC 10118).*

The computation method may be part of the system specifications. Alternately, a cryptographic mechanism identifier template, see 5.4.2, may identify a standard (e.g., ISO/IEC 9797-1) fixing a computation method.

Unless otherwise specified, the following computation method shall be used. Under the control of the key, the algorithm basically converts a current input block of k bytes (typically 8, 16 or 20) into a current output block of the same size."

It is important to stress that the management of keys is critical to secure messaging. What is required is either existing knowledge of shared keys (which many card issuers use) or there exists a supported key agreement mechanism between a terminal and a card to compute a shared secret (or set of shared secrets) for a given transaction.

17.3 Traditional Implementation Examples of Secure Messaging

By way of example there are two widely used implementations in the marketplace today that will illustrate the uses (and options chosen). These examples are:

A. Electronic Passport / International Driver's License

B. GlobalPlatform Secure Channel Protocol

And last, but not least, PIV is also now proposing to use secure messaging.

17.3.1 Electronic Passport / International Driver's License

The electronic passport uses contactless communications only and as such has chosen to protect the communications between a card and a terminal to prevent a third party observer from intercepting said communications for malicious purposes.

17.3.1.1 KEY ESTABLISHMENT

The terminal must first obtain machine readable information printed on the electronic passport or international driver's license. It is this information which is used to calculate the static key used inside the card (for authentication). The protocol also computes session keys derived from the static key for enciphering messages and computing message integrity MACs.

17.3.1.2 ENTITY AUTHENTICATION

For this scheme both terminal and card are authenticated. However it is the successful authentication of the terminal which changes the access conditions on all card data objects protected by the secure messaging protocol.

17.3.1.3 MODE OF SECURE MESSAGING

This scheme uses both enciphered messages and message integrity MACs in both directions (Command and Response).

17.3.2 GlobalPlatform Secure Channel Protocol (SCP)

GlobalPlatform is a cross industry, non-profit association which identifies, develops and publishes specifications that promote the secure and interoperable deployment and management of multiple applications on secure chip technology.

The card specification includes a form of secure messaging known as Secure Channel Protocol (SCP). There are three major protocols published today; specifically SCP 01, SCP 02 and most recently SCP 03.

For easy understanding SCP will be examined at a high level.

17.3.2.1 KEY ESTABLISHMENT

The card key(s) must be known by the (issuer) terminal. GlobalPlatform uses role based entity authentication. Depending on implementation the static keys are either a MASTER key that is used to derive the SCP keys or there is a set of static keys loaded by the issuer. Once the authentication mechanism is performed (and succeeds) session keys are calculated for use in enciphering messages, performing message integrity MACs, and as needed separately enciphering key material sent within a message.

17.3.2.2 ENTITY AUTHENTICATION

For this scheme both terminal and card are authenticated. However it is the successful authentication of the terminal which changes the access conditions on all card data objects protected by the secure messaging protocol. There is one other condition; the lifecycle state of a GlobalPlatform card will determine which mode of communications will be permitted to proceed. (If the lifecycle state is SECURED then only a secure messaging session of MAC or MAC + ENCRYPT modes are permitted).

17.3.2.3 MODE OF SECURE MESSAGING

SCP permits two modes of secure messaging selected by the terminal during the authentication portion of the mechanism:

- **MAC** - The message is not enciphered. Only message integrity MAC is calculated on each command and response.
- **MAC + ENCRYPT** - The command message is enciphered. The response message is usually not enciphered (and is not supported at all in earlier versions of SCP). This is because SCP was designed to primarily send data securely from an issuer terminal into the card.

The following diagram provides an illustration of the protocol flow defined by Global Platform. For details, and definitions of the various acronyms used, refer to section 4.2 of document “GPC_2 2_G_OpacitySecureChannel_v0 1 1 1_ANSIB10.pdf”

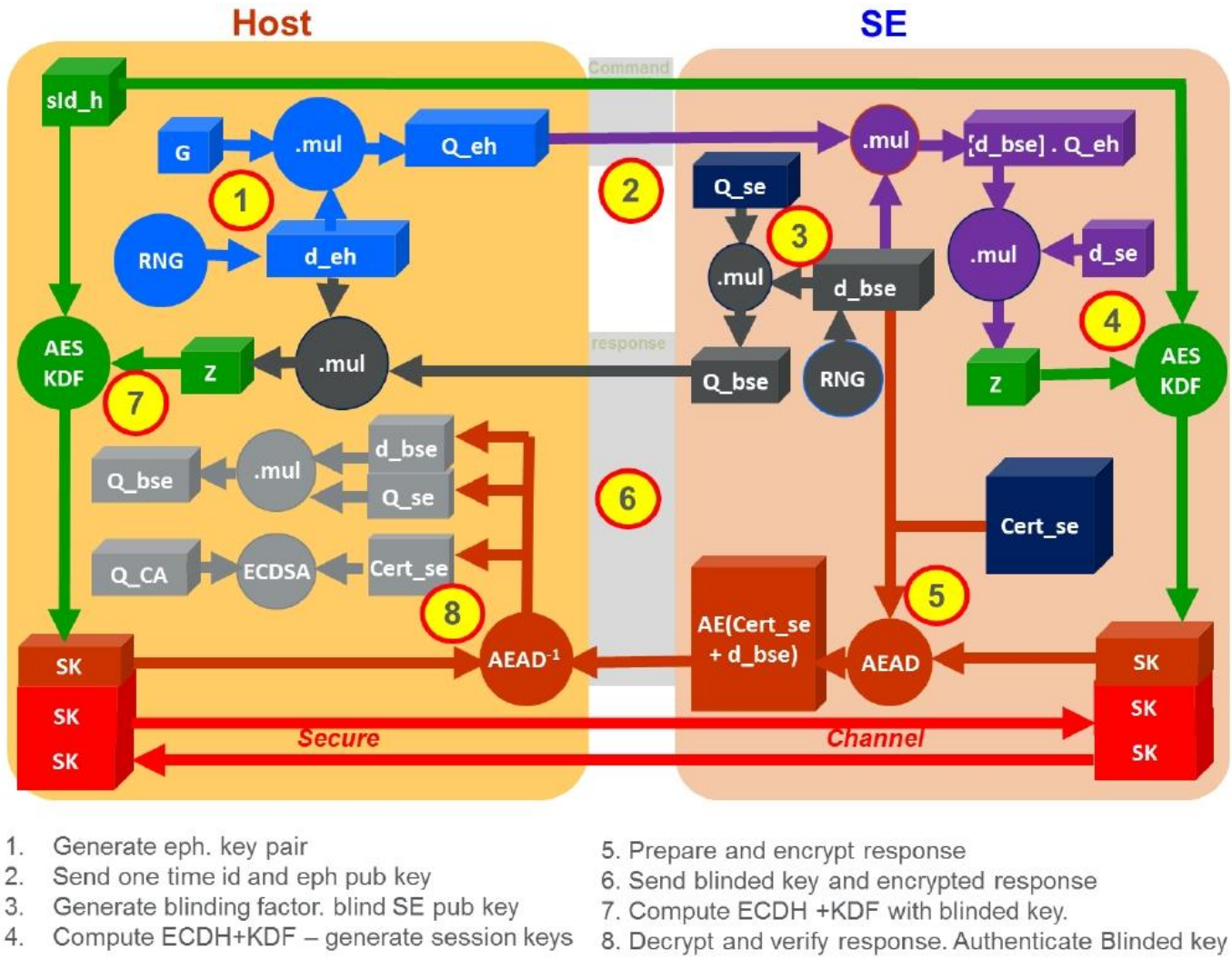


Figure 15. Global Platform - OPACITY Protocol Flow Overview

17.3.3 PIV and Secure Messaging

Per the second draft of SP800-73-4 the Personal Identification Verification (PIV) details an optional secure messaging implementation. This version of secure messaging has several properties that differ from the examples illustrated above.

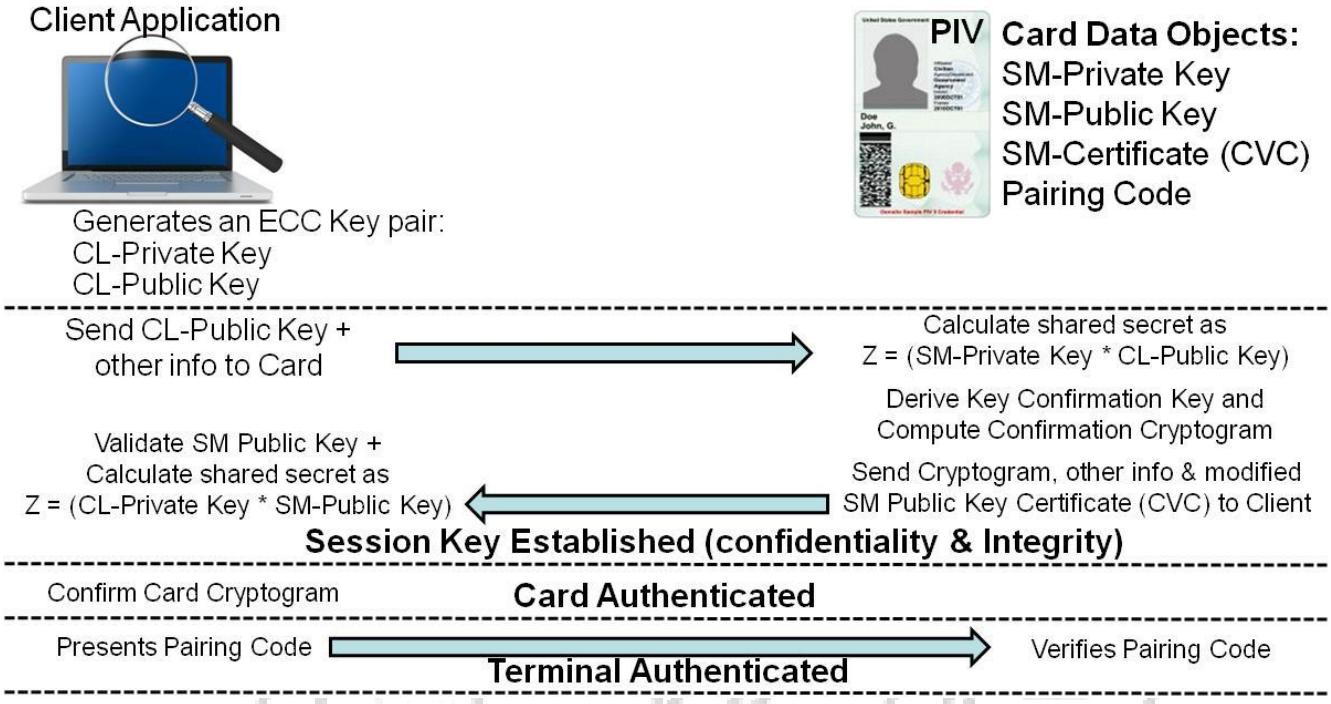


Figure 16. Simplified Diagram of the PIV Secure Messaging Protocol

17.3.3.1 KEY ESTABLISHMENT

A shared secret key is calculated dynamically from asymmetric Elliptic Curve key pairs; an ephemeral (short life transient) key pair of the terminal and a static key pair inside the card signed by the Issuer. The protocol also computes session keys for authentication of the card, enciphering messages and computing message integrity MACs.

A symmetric shared secret key "Z" is calculated independently on the terminal and in the card based on information passed by one party to the other party. For Z to be calculated the terminal and card are obliged to exchange their respective Elliptic Curve public key with the other party.

The mathematics of this shared secret calculation can be illustrated through an example below. This example uses the "ephemeral – static" form of Elliptic curve cryptography per SP800-56A Revision 2 Section 6.2.2. This protocol type is also known as a cofactor one-pass Diffie Hellman scheme.

- *Step 0 (picked as part of the scheme): The Client and the PIV Card have already agreed on an ECC curve and base point G on that curve. Base point G can be expressed as (x-value, y-value). The PIV Card has a Secure Messaging (SM) Private-Public key pair certified by its issuing authority.*
- *Step 1a: The client generates a random integer <CL-Private key> which is its Private Key.*
- *Step 1b: The client computes its Public Key <CL-Public Key>=<CL-Private Key>*G (i.e. G added to itself <CL-Private Key> times).*

- *Step 1c: The PIV Card uses it's Certificate Authority assigned static Private Key integer <SM-Private Key> and static Public Key <SM-Public Key>=<SM-Private Key>*G.*
- *Step 2: The Client and the PIV Card exchange public ECC keys (<CL-Public Key> and <SM-Public key> respectively) along with other information to be used later in the protocol to derive session keys.*
- *Step 3a: The Client calculates their shared secret Z = <Cl-Private Key>*< SM-Private Key>*G.. (Only the x-axis value of Point G is used)*
- *Step 3b: The PIV Card calculates their shared secret Z = <SM-Private Key>*<CL-Private Key>*G. (Only the x-axis value of Point G is used)*

*This works because (Client-Private Key * PIV Card-Public Key) = (PIV Card-Private Key * Client-Public Key) since both parties use the same base point G.*

The shared secret Z is then used, along with other shared or known information, to create session keys. These session keys are the Key Confirmation Session Key, Encryption Session Key, Command MAC Session Key and Response MAC Session key).

For security reasons, the card is obliged in this protocol to generate a cryptogram as the card Elliptic Curve key pairs are static. The card computes this cryptogram using the Key Confirmation Session Key. The card sends this cryptogram to the terminal so the terminal can verify the card cryptogram was correctly computed (which validates the shared secret Z calculation done by the card). This validation also authenticates the card to the terminal.

17.3.3.2 ENTITY AUTHENTICATION

This scheme only authenticates the card to the terminal.
In other words, access conditions for those data objects protected by secure messaging are changed as a result of key establishment in this protocol; NOT by authenticating the terminal as used in other secure messaging implementations.

17.3.3.3 MODE OF SECURE MESSAGING

This scheme uses both enciphered messages and message integrity MACs in both directions (Command and Response).

18 Acknowledgements

This document was developed by the Smart Card Alliance for the Certified Smart Card Industry Professional (CSCIP) program. Publication of this document by the Smart Card Alliance does not imply the endorsement of any of the member organizations of the Alliance.

About LEAP and the CSCIP Program

The Smart Card Alliance Leadership, Education and Advancement Program (LEAP) was formed to: offer a new individual members-only organization for smart card professional; advance education and professional development for individuals working in the smart card industry; manage and confer, based on a standardized body-of-knowledge examination, the Certified Smart Card Industry Professional (CSCIP) designation.

LEAP members who wish to achieve certification as experts in smart card technology may do so at any time. Certification requires that LEAP members meet specific educational and professional criteria prior to acceptance into the certification program.

A series of educational modules forming the CSCIP certification body of knowledge has been developed by leading smart card industry professionals and is updated regularly. These educational modules prepare applicants for the multi-part CSCIP exam administered by the Smart Card Alliance. The exam requires demonstrated proficiency in a broad body of industry knowledge, as opposed to expertise in specialized smart card disciplines. Applicants must receive a passing grade on all parts of the exam to receive the CSCIP certification.

LEAP membership in good standing is required to sustain the certification, and documentation of a required level of continuing education activities must be submitted every three years for CSCIP re-certification.

Additional information on LEAP and the CSCIP accreditation program can be found at http://www.smartcardalliance.org.

Trademark Notice