FIPS PUB 201-2

Deleted: 1

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Personal Identity Verification (PIV)
of
Federal Employees and Contractors
DRAFT

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8900

March 2011

Deleted: 2006

U.S. DEPARTMENT OF COMMERCE
Gary Locke, Secretary

Deleted: *Carlos M. Gutierrez*

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Dr. Patrick D. Gallagher, Director

Deleted: *William A. Jeffrey*

Acknowledgements

NIST would like to acknowledge the significant contributions of the Federal Identity Credentialing Committee (FICC), Identity, Credential, and Access Management Subcommittee (ICAMSC), and the Smart Card Interagency Advisory Board (IAB) for providing valuable contributions to the development of technical frameworks on which this standard is based.

Special thanks to those who have participated in the business requirements meeting and provided valuable comments in shaping this standard.

Deleted:)

Deleted: workshops

Deleted: technical suggestions

Deleted: NIST also acknowledges the comments received from government and industry organizations during the preliminary draft review period.

FOREWORD

The Federal Information Processing Standards Publication Series of the National Institute of Standards and Technology (NIST) is the official series of publications relating to standards and guidelines adopted and promulgated under the provisions of the Federal Information Security Management Act (FISMA) of 2002.

Comments concerning FIPS publications are welcomed and should be addressed to the Director, Information Technology Laboratory, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900.

Cita Furlani, Director
Information Technology Laboratory

Deleted: Dr. Shashi Phoha

ABSTRACT

This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems.

The standard contains the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including identity proofing, registration, and issuance. The standard also provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, *Interfaces for Personal Identity Verification*. The interfaces and data formats of biometric information are specified in Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*. The requirements for cryptographic algorithms are specified in the Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the accreditation of the PIV Card issuer are specified in the Special Publication 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers (PCI's)*. The unique organizational codes for Federal agencies are assigned in the Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*.

This standard does not specify access control policies or requirements for Federal departments and agencies.

Deleted: two major sections. Part one describes

Deleted: personal

Deleted: Part two

Deleted: Similarly,

Keywords: Architecture, authentication, authorization, biometrics, credential, cryptography, Federal Information Processing Standards (FIPS), HSPD-12, identification, identity, infrastructure, model, Personal Identity Verification, PIV, validation, verification.

Federal Information Processing Standards 201
2011

Deleted: 2005¶

Announcing the
Standard for

Personal Identity Verification
of
Federal Employees and Contractors
DRAFT

Federal Information Processing Standards Publications (FIPS PUBS) are issued by the National Institute of Standards and Technology (NIST) after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act (FISMA) of 2002.

1. Name of Standard.

FIPS PUB 201-2: Personal Identity Verification (PIV) of Federal Employees and Contractors.[1]

2. Category of Standard.

Information Security.

3. Explanation.

Homeland Security Presidential Directive 12 (HSPD-12), dated August 27, 2004, entitled "Policy for a Common Identification Standard for Federal Employees and Contractors," directed the promulgation of a Federal standard for secure and reliable forms of identification for Federal employees and contractors. It further specified secure and reliable identification that—

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

The directive stipulated that the standard include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. As promptly as possible, but in no case later than eight months after the date of promulgation, executive departments and agencies are required to implement the standard for identification issued to Federal employees and contractors in gaining physical access to controlled facilities and logical access to controlled information systems.

[1] This standard is in response to the Homeland Security Presidential Directive-12 which states that it is "intended only to improve the internal management of the executive branch of the Federal Government".

4. Approving Authority.

Secretary of Commerce.

5. Maintenance Agency.

Department of Commerce, NIST, Information Technology Laboratory (ITL).

6. Applicability.

This standard is applicable to identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems except for "national security systems" as defined by 44 U.S.C. 3542(b)(2). Except as provided in HSPD-12, nothing in this standard alters the ability of government entities to use the standard for additional applications.

Special-Risk Security Provision—The U.S. Government has personnel, facilities, and other assets deployed and operating worldwide under a vast range of threats (e.g., terrorist, technical, intelligence), particularly heightened overseas. For those agencies with particularly sensitive OCONUS threats, the issuance, holding, and/or use of PIV credentials with full technical capabilities as described herein may result in unacceptably high risk. In such cases of extant risk (e.g., to facilities, individuals, operations, the national interest, or the national security), by the presence and/or use of full-capability PIV credentials, the head of a Department or independent agency may issue a select number of maximum security credentials that do not contain (or otherwise do not fully support) the wireless and/or biometric capabilities otherwise required/referenced herein. To the greatest extent practicable, heads of Departments and independent agencies should minimize the issuance of such special-risk security credentials so as to support inter-agency interoperability and the President's policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective security technology advances, the need for this provision will be re-assessed as the standard undergoes the normal review and update process.

7. Specifications.

Federal Information Processing Standards (FIPS) 201 Personal Identity Verification (PIV) of Federal Employees and Contractors.

8. Implementations.

The PIV standard satisfies the control objectives, security requirements, and technical interoperability requirements of HSPD-12. The PIV standard specifies implementation of identity credentials on integrated circuit cards for use in a Federal personal identity verification system.

A PIV Card must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification.

Federal departments and agencies must use accredited issuers to issue identity credentials for Federal employees and contractors. For this purpose, NIST provided guidelines for the accreditation of PIV Card issuers in [SP 800-79]. NIST also developed a PIV Validation Program that tests implementations for

Deleted: this

Deleted: consists of two parts—PIV-I and PIV-II. PIV-I

Deleted: and meets the

Deleted: of HSPD 12, while PIV-II meets the

Deleted: -II

Deleted: and use

Deleted: Cards

Deleted: may self-accredit, or

Deleted: other

Deleted: ,

Deleted: until a government-wide PIV-II

Deleted: process is established. The standard

Deleted: covers security and interoperability requirements for PIV Cards. Funding permitting, NIST plans to develop

Deleted: will test

conformance with this standard, and specifically with [SP 800-73]. Additional information on this program is published and maintained at http://csrc.nist.gov/groups/SNS/piv/npivp/.

The Office of Management and Budget (OMB) provides an implementation oversight of this standard. The respective numbers of agency-issued 1) general credentials and 2) Special-risk credentials (issued under the Special-Risk Security Provision) are subject to annual reporting to the OMB under the annual reporting process in a manner prescribed by OMB.

Deleted: .

Deleted: will be

Deleted: http://csrc.nist.gov/npivp/ as it becomes available.

Deleted: shall be

Deleted: Office of Management and Budget (

Deleted:)

9. Effective Date.

This standard is effective immediately. Federal departments and agencies shall meet the requirements of this standard in accordance with the timetable specified by OMB. OMB has advised NIST that it plans to issue guidance regarding the adoption and implementation of this standard.

Deleted: PIV-I no later than October 27, 2005,

Deleted: in HSPD 12. The

Deleted: transition from PIV-I to PIV-II. It is anticipated that some Federal departments

Deleted: agencies may begin with PIV-II, which would eliminate the need for such a transition.

10. Qualifications.

The security provided by the PIV system is dependent on many factors outside the scope of this standard. Upon adopting this standard, organizations must be aware that the overall security of the personal identification system relies on—

- Assurance provided by the issuer of an identity credential that the individual in possession of the credential has been correctly identified
- Protection provided to an identity credential stored within the PIV Card and transmitted between the card and the PIV issuance and usage infrastructure
- Protection provided to the identity verification system infrastructure and components throughout the entire life cycle.

Although it is the intent of this standard to specify mechanisms and support systems that provide high assurance personal identity verification, conformance to this standard does not assure that a particular implementation is secure. It is the implementer's responsibility to ensure that components, interfaces, communications, storage media, managerial processes, and services used within the identity verification system are designed and built in a secure manner.

Similarly, the use of a product that conforms to this standard does not guarantee the security of the overall system in which the product is used. The responsible authority in each department and agency shall ensure that an overall system provides the acceptable level of security.

Because a standard of this nature must be flexible enough to adapt to advancements and innovations in science and technology, the NIST has a policy to review this standard within five years to assess its adequacy.

Deleted: will

Deleted: NIST plans to seek agency input in one year to see whether a full review of the standard is needed.

11. Waivers.

As per the Federal Information Security Management Act of 2002, waivers to Federal Information Processing Standards are not allowed.

12. Where to Obtain Copies.

This publication is available through the Internet by accessing http://csrc.nist.gov/publications/.

13. Patents.

Aspects of the implementation of this standard may be covered by U.S. or foreign patents.

Table of Contents

List of Appendices

List of Figures

List of Tables

Deleted: ¶
Page Break
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
[This page intentionally left blank.]¶

1. Introduction

Authentication of an individual's identity is a fundamental component of physical and logical access control processes. When an individual attempts to access security-sensitive buildings, computer systems, or data, an access control decision must be made. An accurate determination of an individual's identity is needed to make sound access control decisions.

A wide range of mechanisms is employed to authenticate identity, utilizing various classes of identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper or other non-automated, hand-carried credentials, such as driver's licenses and badges. Access authorization to computers and data has traditionally been based on identities authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been used in physical and logical security applications, replacing or supplementing the traditional identity credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential. This document establishes a standard for a Personal Identity Verification (PIV) system based on secure and reliable forms of identity credentials issued by the Federal government to its employees and contractors. These credentials are intended to authenticate individuals who require access to Federally controlled facilities, information systems, and applications. This standard addresses requirements for initial identity proofing, infrastructures to support interoperability of identity credentials, and accreditation of organizations and processes issuing PIV credentials.

Deleted: identification

1.1 Purpose

This standard defines a reliable, government-wide identity credential for use in applications such as access to Federally controlled facilities and information systems. This standard has been developed within the context and constraints of Federal law, regulations, and policy based on information processing technology currently available and evolving.

Deleted: PIV system

This standard specifies a PIV system within which a common identity credential can be created and later used to verify a claimed identity. The standard also identifies Federal government-wide requirements for security levels that are dependent on risks to the facility or information being protected.

Deleted: identification credentials

1.2 Scope

Homeland Security Presidential Directive 12 [HSPD-12], signed by the President on August 27, 2004, established the requirements for a common identification standard for identity credentials issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standards (FIPS) publication to define such a common identity credential. In accordance with HSPD-12, this standard defines the technical requirements for the identity credential that—

Deleted: identification

Deleted: identification

- Is issued based on sound criteria for verifying an individual employee's identity
- Is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
- Can be rapidly authenticated electronically

- Is issued only by providers whose reliability has been established by an official accreditation process.

This 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. This standard does not specify access control policies or requirements for Federal departments and agencies. Therefore, the scope of this standard is limited to authentication of an individual's identity. Authorization and access control decisions are outside the scope of this standard. Moreover, requirements for a temporary card used until the new PIV Card arrives are out of scope of this standard.

Deleted: Access authorization

1.3 Change Management

Every new revision of this standard introduces refinements and changes that may impact existing implementations. FIPS 201 and its normative specifications encourage implementation approaches that reduce the high cost of configuration and change management by architecting resilience to change into system processes and components. Nevertheless, changes and modifications are introduced. Because of the importance of this issue, the Change Management section has been added to the standard.

This section provides change management principles and guidance to manage newly introduced changes and modifications to the previous version of this standard. Specifically, this section provides a description of the types of changes expected in FIPS 201 revisions.

1.3.1 Backward compatible change

A backward compatible change is a change or modification to an existing feature that does not break the systems using this feature. For example, changing the NACI indicator from mandatory to optional in the PIV Authentication certificate does not affect the systems using the PIV Authentication certificate for PIV authentication (i.e., using the PKI-PIV mechanism).

1.3.2 Non-backward compatible change

A non-backward compatible change is a change or modification to an existing feature such that the modified feature cannot be used with existing systems. For example, changing the format of the biometric data would not be compatible with the existing system, because a biometric authentication attempt with the modified format would fail. Similarly, changing the PIV Card Application IDentifier (AID) would introduce a non-backward compatible change. As a result, all systems interacting with the PIV card would need to be changed to accept the new PIV AID.

1.3.3 New Features

New features are optional or mandatory features that are added to the standard. New features do not interfere with backward compatibility because they are not part of the existing systems. For example, the addition of an optional On-Card Biometric comparison (OCC) authentication mechanism is a new feature that does not affect the features in the current systems. The systems will need to be updated if an agency decides to support the OCC authentication mechanism.

1.3.4 Deprecated and removed

When a feature is discontinued or no longer needed, it is deprecated. Such a feature remains in the current standard as an optional feature but its use is strongly discouraged. A deprecated feature does not

affect existing systems but should be phased out in future systems, because the feature will be removed in the next revision of the standard. For example, existing PIV Cards with deprecated data elements remain valid until they naturally expire. Replacement PIV Cards, however, should not re-use the deprecated features because the next revision of the standard will remove the support for deprecated data elements.

1.3.5 FIPS 201 Version Management

Subsequent revisions of this standard may necessitate FIPS 201 version management that introduces new version numbers for FIPS 201 products. Components that may be affected by version management include, for example, PIV Cards, PIV middleware software, and card issuance systems.

New version numbers may be assigned in [SP 800-73] depending on the nature of the change. For example, new mandatory features introduced in a revision of this standard, may necessitate a new PIV card application version number so that systems can quickly discover the new mandatory features. Optional features, on the other hand, may be discoverable by an on-card discovery mechanism.

1.4 Document Organization

This standard describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD-12, including identity proofing, registration, and issuance. It provides detailed technical specifications to support the control and security objectives of HSPD-12 as well as interoperability among Federal departments and agencies. This standard describes the policies and minimum requirements of a PIV Card that allows interoperability of credentials for physical and logical access. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in NIST Special Publication 800-73 [SP 800-73], *Interfaces for Personal Identity Verification*. Similarly, the requirements for collection and formatting of biometric information are specified in NIST Special Publication 800-76 [SP 800-76], *Biometric Data Specification for Personal Identity Verification*. The requirements for cryptographic algorithms are specified in the Special Publication 800-78 [SP 800-78], *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the accreditation of PIV Card issuers are specified in the Special Publication 800-79 [SP 800-79], *Guidelines for the Accreditation of Personal Identity Verification Card Issuers (PCI's)*. The unique organizational codes for Federal agencies are assigned in the Special Publication 800-87 [SP 800-87], *Codes for the Identification of Federal and Federally-Assisted Organizations*. The requirements for the PIV Card reader are provided in Special Publication 800-96 [SP 800-96], *PIV Card to Reader Interoperability Guidelines*.

Deleted: is composed of two parts, PIV-I and PIV-II. The first part (PIV-I)

Deleted: personal

Deleted: , but does not address the interoperability of PIV Cards and systems among departments and agencies. ¶ The second part (PIV-II)

Deleted: in PIV-I

Deleted: PIV-II

Deleted: access

Deleted: (

Deleted:),

Deleted: (SP 800-76), Biometric Data Specification for Personal Identity Verification

All sections in this document are *normative* (i.e., mandatory for compliance) unless specified as *informative* (i.e., non-mandatory). Following is the structure of this document:

- Section 1, Introduction, provides background information for understanding the scope of this standard. This section is *informative*.
- Section 2, Common Identification, Security, and Privacy Requirements, outlines the requirements for identity proofing, registration, and issuance, by establishing the control and security objectives for compliance with HSPD-12. This section is *normative*.
- Section 3, PIV System Overview, serves to provide a PIV system overview. This section is *informative*.

Deleted: PIV-I

- Section 4, PIV Front-End Subsystem, provides the requirements for the components of the PIV front-end subsystem. Specifically, this section defines requirements for the PIV Card, logical data elements, biometrics, cryptography, and card readers. This section is *normative*.
- Section 5, PIV Key Management Requirements, defines the processes and components required for managing PIV Card life cycle. It also provides the requirements and specifications related to this subsystem. This section is *normative*.
- Section 6, PIV Cardholder Authentication, defines a suite of identity authentication mechanisms that are supported by the PIV Card, and their applicability in meeting the requirements of graduated levels of identity assurance. This section is *normative*.
- Appendix A, PIV Validation, Certification, and Accreditation, provides additional information regarding compliance with this document. This appendix is *normative*.
- Appendix B, Background Check Descriptions, provides the requirements for background checks. This appendix is *informative*.
- Appendix C, PIV Card Processes, provides the summary of requirements for PIV card issuance and maintenance processes. This appendix is *informative*.
- Appendix D, PIV Object Identifiers and Certificate Extension, provides additional details for the PIV objects identified in Section 4. This appendix is *normative*.
- Appendix E, Glossary of Terms, Acronyms, and Notations, describes the vocabulary and textual representations used in the document. This appendix is *informative*.
- Appendix F, References, lists the specifications and standards referred to in this document. This appendix is *informative*.
- Appendix G, Revision History, lists changes made to this standard from its inception. This appendix is *informative*.

Deleted: Card Issuance and

Deleted: Subsystem

Deleted: and processes that are part of the PIV-II

Deleted: Card

Deleted: Processes, provides two models for identity proofing, registration, issuance, and maintenance of identity credentials. This section is *informative*.¶ Appendix B, PIV

Deleted: guidance for the

Deleted: C

Deleted: section

Deleted: Physical Access Control Mechanisms, discusses the Physical Access Control Systems (PACS) assurance profiles and maps them to the FIPS 201 assurance levels. This section is *informative*.¶ Appendix F,

Deleted: and

Deleted: section

Deleted: G

Deleted: section

Deleted: ¶
Section Break (Next Page)
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
PART 1: PIV-I¶
¶
¶
This part describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD 12, including the personal identity proofing process.¶
Implementation Timeframe: In accordance with HSPD 12, departments and agencies shall meet the requirements of this part no later than eight months following promulgation of the standard.¶
¶
¶

2. Common Identification, Security, and Privacy Requirements

This section addresses the fundamental control and security objectives outlined in HSPD-12, including the identity proofing requirements for Federal employees and contractors.

Deleted: provides the requirements for the first part of the standard. PIV-I

Deleted: personal

Deleted: process

Deleted: Note that PIV-I does not address interoperability of PIV credentials and systems among agencies or compel the use of a single, universal credential.

2.1 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 true 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 is initiated and the FBI National Criminal History Check (NCHC) is completed;

Deleted: <#>Only an individual with a background investigation on record is issued a credential;¶

+ 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;

Deleted: valid

+ 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 modified, duplicated, or forged.

2.2 Credentialing Requirements

Federal departments and agencies shall use the Credentialing guidance as contained in a memorandum dated July 31, 2008, from Linda M. Springer, the Director of the Office of Personnel Management, to Heads of Departments and Agencies when determining whether to issue or revoke PIV Cards. [SPRINGER MEMO]

2.3 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 approved identity proofing and registration process in accordance with [SP 800-79].

+ The process shall begin with initiation of a NACI or equivalent. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. Also, the FBI NCHC (fingerprint check) shall be completed before credential issuance. Appendix B, Background Check Descriptions, provides further details on NACI.

+ The applicant shall appear in-person at least once before the issuance of a PIV credential.

+ During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form. The primary identity source document shall be neither expired nor cancelled, shall be one of the following forms of identification:

  – A U.S. Passport or a U.S. Passport Card;
  – Permanent Resident Card or Alien Registration Receipt Card (Form I-551)
  – Foreign passport that contains a temporary I-551 stamp or temporary I-551 printed notation on a machine-readable immigrant visa
  – Employment Authorization document that contains a photograph (Form I-766)
  – In the case of a nonimmigrant alien authorized to work for a specific employer incident to status, a foreign passport with Form I-94 or Form I-94A bearing the same name as the passport and containing an endorsement has not yet expired and the proposed employment is not in conflict with any restrictions or limitations identified on the form
  – Passport from the Federal States of Micronesia (FSM) or the Republic of the Marshall Islands (RMI) with Form I-94 or Form I-94A indicating nonimmigrant admission under the Compact of Free Association Between the US and the FSM or RMI
  – 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 Department of Defense Common Access Card.

Deleted: For compliance with the PIV-I control objectives,

Deleted: identity credentials

Deleted: .

Deleted: National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment.

Deleted: At a minimum

Deleted: National Criminal History Check

Deleted: Beginning with Part 2, 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.

Deleted: C

Deleted: NAC and

Deleted: must

Deleted: documents must come from the list of acceptable documents included in *Form I-9, OMB No. 1115-0136, Employment Eligibility Verification*. At least one

Deleted: a valid State or Federal government-issued picture

Deleted: (ID).

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 any 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 School ID with 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 ID Card for use of Resident Citizen in the United States (Form I-179);
- A Certification of Birth or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350);
- Unexpired Temporary Resident Card (Form I-688);
- Unexpired Employment Authorization Card (Form I-688A);
- Unexpired Reentry Permit (Form I-327);
- Unexpired Refugee Travel Document (Form I-571);
- Unexpired employment authorization document issued by Department of Homeland Security (DHS);
- Unexpired 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, and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.

+ A new chain-of-trust record shall be created in accordance with Section 4.4.1 for the applicant.

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 of the Federal department or agency.

Deleted: Two examples of processes that meet these requirements are provided in Appendix A, PIV Processes.

These identity proofing requirements also apply to citizens of foreign countries who are working for the Federal government overseas. However, a process for registration and approval 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.

2.4 PIV Card Issuance Requirements

Departments and agencies shall meet the requirements defined below when issuing identity credentials. The issuance process used when issuing credentials shall be accredited by the department as satisfying the requirements below and approved in writing by the head of the Federal department or agency.

- Credentials 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].
- The process shall ensure the initiation of a NACI or equivalent or the location of a completed and successfully adjudicated NACI or equivalent. The process shall also ensure the FBI NCHC is completed before issuing an identity credential. The PIV credential shall be revoked if the results of the investigation so justify.
- Biometrics used to personalize the PIV Card must be taken from the card issuer's chain-of-trust for the applicant.
- During the issuance process, the issuer shall verify that the individual to whom the credential 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 the biometric included in the PIV Card. The 1:1 biometric match requires either a match of fingerprint(s) or a match of iris image(s). 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.
- 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).
- The PIV Card shall be valid for no more than six years.

Cards that contain topographical defects (e.g., scratches, poor color, fading, etc), contain errors in optional fields, are not properly printed, or are not delivered to the cardholder are not considered PIV Issued Cards. PIV Card issuer is responsible for the card stock, its management, and its integrity. This standard does not place any requirements on these cards. Agencies may reuse them or discard them, as they deem appropriate.

2.4.1 Special Rule for Pseudonyms

In limited circumstances Federal employees are permitted to use pseudonyms during the performance of their official duties with the approval of their employing agency. (See, for example, Section 1.2.4 of the Internal Revenue Service Manual, which authorizes approval by an employee's supervisors of the use of a pseudonym to protect the employee's personal safety. Section 1.2.4.6.6 of the Manual provides that

Deleted: and Maintenance

Deleted: For compliance with the PIV-I control objectives,

Deleted: and maintenance

Deleted: Two examples of processes that meet these requirements are provided in Appendix A.

Deleted: and maintenance

Deleted: .

Deleted: completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (

Deleted:),

Deleted: other OPM

Deleted: National Security community investigation as required for Federal employment

Deleted: At the time of issuance,

Deleted: (and on whom the background investigation was completed)

employees authorized to use a pseudonym in the course of their official duties will be "given a new ID Card with a new ID number", which will also serve as the employee's building pass.) In instances where an agency has formally authorized the use of a pseudonym, the card issuer shall issue a PIV Card to the employee using the agency-approved employee pseudonym. The issuance of a PIV Card using a pseudonym shall follow the procedures in PIV Card Issuance Requirements for employee name changes except that the employee must provide evidence satisfactory to the card issuer that the pseudonym is authorized by the employee's agency.

2.4.2 Grace Period

In some instances an individual's status as a Federal employee or contractor will lapse for a brief time period. In instances where such an interregnum does not exceed 60 days, a card issuer shall issue the employee or contractor a new PIV Card in a manner consistent with PIV Card Issuance.

2.5 PIV Card Maintenance Requirements

The PIV Card shall be maintained using processes that comply with this section.

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. The PIV system should ensure that this information is distributed effectively within the PIV management infrastructure. Background Investigation status information shall be made available to authenticating parties, government-wide, through the Office of Personnel Management (OPM) Central Verification System, Backend Attribute Exchange, or other operational system approved by OMB. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card maintenance.

2.5.1 PIV Card Renewal Requirements

Renewal is the process by which a valid PIV Card is replaced without the need to repeat the entire identity proofing and registration procedure. The original PIV Card must be surrendered when requesting a renewal. The PIV Card is renewed only after a proper authority has authorized renewal of the credential. The issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials for current employees, the NACI check shall be followed in accordance with OPM guidance. The issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or a match of iris image(s). Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. The entire identity proofing and registration is required if a cardholder’s chain-of-trust record is not available.

A cardholder shall be allowed to apply for a renewal starting twelve weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card. The cardholder will not be allowed to start the renewal process if the original PIV Card is expired. The original PIV Card must be collected and destroyed. If there is any data change about the cardholder, the issuer will record this in the chain-of-trust and distribute the changed data within the PIV management infrastructure. If the changed data is the cardholder’s name, then the issuer shall meet the requirements in Section 2.5.2.1, Special Rule for Name Change by Cardholder.

The same biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than twelve years after the date that the biometric data was obtained. The digital signature must be recomputed with the new FASC-N.

The expiration date of the PIV Authentication Key certificate, Card Authentication Key certificate, and optional Digital Signature Key certificate shall not be later than the expiration date of the PIV Card. Hence, a new PIV Authentication Key and certificate and a new asymmetric Card Authentication Key and certificate shall be generated. Key Management key(s) and certificate(s) may be imported to the new PIV Card.

2.5.2 PIV Card Reissuance Requirements

A cardholder shall apply 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.

In case of reissuance, the complete registration and issuance process is not required if the applicant for reissuance can be reconnected to the chain-of-trust record. Reconnecting to the chain-of-trust requires a 1:1 biometric match against the biometric reference data held in a chain-of-trust (see Section 4.4.1). The 1:1 biometric match requires either a match of fingerprint(s) or a match of iris image(s). Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. The card issuer shall verify that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials. The entire identity proofing and registration is required if a cardholder's chain-of-trust record is not available.

When reissuing a PIV Card, normal operational procedures must be in place to ensure the following:

- The PIV Card itself is revoked. Any local databases that contain FASC-N values must be updated to reflect the change in status.
- The CA shall be informed and the certificates corresponding to the PIV Authentication Key and asymmetric Card Authentication Key on the PIV Card shall be revoked. Revocation of the Digital Signature Key certificate is only optional if the PIV Card has been collected and zeroized or destroyed. Similarly, the Key Management Key certificate should also be revoked if there is risk that the private key was compromised. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers.
- Online Certificate Status Protocol (OCSP) responders shall 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 PIV Card shall be collected and destroyed if possible. If the card cannot be collected, normal operational procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures must be executed to disseminate the information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.

If the expiration date of the reissued PIV Card is later than the expiration date of the old card, the card issuer shall ensure a proper authority has authorized reissuance of the credential and the NACI check is followed in accordance with OPM guidance. The same biometric data may be reused with the new PIV

Card if the expiration date of the new PIV Card is no later than twelve years after the date that the biometric data was obtained.

2.5.2.1 Special Rule for Name Change by Cardholder

Name changes are a frequent occurrence. People's names often change as a result of marriage or divorce. Less frequently, people change their names as a matter of personal preference. In the event that a cardholder notifies a card issuer that his or her name has changed, and presents the card issuer with evidence of a formal name change, such as a marriage certificate, a divorce decree, judicial recognition of a name change, or other mechanism permitted by State law or regulation, the card issuer shall issue the cardholder a new card following the procedures set out in Section 2.5.2, PIV Card Reissuance. Also, the card issuer shall update the chain-of-trust record to include the evidence of a formal name change.

2.5.3 PIV Card Re-Key Requirements

There may be instances where keys on the PIV Card or in the PIV System are compromised and the issuer is required to replace the keys on the PIV Card with new ones. The cardholder data and any other related data on the card shall not be changed. Only the keys and certificates shall be updated.

2.5.4 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. The Post Issuance update applies to cases where one or more certificates, keys, biometric data objects, or signed data objects are updated. The PIV Card expiration date or the FASC-N shall not be modified by a Post Issuance update.

A PIV Card post issuance update may be done locally (performed with the issuer in physical custody of the PIV Card) or remotely (performed with the PIV Card at a remote location). Post issuance updates shall be performed with issuer security controls equivalent to those applied during PIV Card reissuance. For remote post issuance updates, the following shall apply:

- Communication between the PIV Card issuer and the PIV Card shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules (one being the PIV Card).
- Data transmitted between the PIV Card issuer and PIV Card shall be encrypted and contain data integrity checks.
- The PIV Card will communicate with no end point entity other than the PIV Card issuer during the remote post issuance update.
- If the PIV Card post issuance update begins[2] but fails for any reason, the PIV Card issuer shall immediately terminate the PIV Card as described in Section 2.5.6, and a diligent attempt shall be made to collect and destroy the PIV Card.

Post issuance updates to biometric data objects, other than to the digital signature blocks within the biometric data objects, shall satisfy the requirements for verification data reset specified in Section 2.5.5.

[2] A post issuance update has "begun" if the PIV Card Issuer has established the mutually authenticated session to the PIV Card and the PIV Card Issuer has sent any command to the PIV Card that could modify the persistent state of the PIV Card.

2.5.5 PIV Card Verification Data Reset

The PIN on a PIV Card may need to be reset if the cardholder wants to change their PIN, 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. PIN resets may be performed by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card.[3] Departments and agencies may adopt more stringent procedures for PIN reset (including requiring in-person appearance or disallowing PIN reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency.

Verification data other than the PIN may also be reset (i.e., re-enrollment) by the card issuer. Before the reset PIV Card is provided back to the cardholder, the card issuer shall either ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card or the biometric in the cardholder's chain-of-trust (see Section 4.4.1), or require the cardholder to provide a primary identity source document (see Section 2.3). If a biometric match is performed, then the type of biometric used for the match shall not be the same as the type of biometric data that is being reset. Departments and agencies may adopt more stringent procedures for verification data reset (including disallowing verification data reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented by each department and agency.

2.5.6 PIV Card Termination Requirements

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

- A Federal employee separates (voluntarily or involuntarily) from Federal service
- An employee of a Federal contractor separates (voluntarily or involuntarily) from their employer
- 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 values must be updated to reflect the change in status.
- The CA shall be informed and the certificates corresponding to PIV Authentication Key and the asymmetric Card Authentication Key on the PIV Card must be revoked. Departments and

[3] If no biometric data could be collected from the cardholder then the cardholder may instead provide a primary identity source document (see Section 2.3).

agencies may revoke certificates corresponding to the optional Digital Signature and Key Management keys. CRLs issued shall include the appropriate certificate serial numbers.

+ OCSP responders shall 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 IIF collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.

A summary of PIV Card Issuance and PIV Card Maintenance requirements is provided in Appendix C.

2.6 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 Office of Management and Budget (OMB) Memorandum M-03-22 [OMB322], 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 the PIV 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 life cycle:

Deleted: of applicants, departments and agencies shall do the following

+ Assign an individual to the role of senior agency official for privacy. The senior agency official for privacy 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.

Deleted: may

+ Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with methodology of [E-Gov] and the requirements of [OMB322]. 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, personally identifiable 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).

Deleted: personal information in

Deleted: form [IIF]),

Deleted: .

+ PIV applicants shall be provided full disclosure of the intended uses of the PIV credential 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.[4]
- 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 NIST SP 800-53 [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 information in identifiable form. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV Card.

Deleted: IIF

Deleted: IIF

Deleted: IIF

Deleted: ,

Deleted: [SP800-53]

Deleted: credential

Deleted: ¶
¶
Section Break (Next Page)
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
PART 2: PIV-II¶
¶
¶
This part of the document and its referenced supporting publications provide detailed technical specifications of components and processes required for interoperability of PIV Cards with the personal authentication, access control, and PIV card management systems across the Federal government.¶
Implementation Timeframe: OMB has advised NIST that it plans to issue guidance regarding department and agency development of transition plans to PIV-II.¶

[4] Agencies may refer to NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), for a best practice guideline on protection of PII.

3. PIV System Overview

A notional PIV system architecture is presented in this section. 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 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 identity 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 life cycle activities of the PIV Card.

Deleted: This section provides the background for the PIV-II requirements identified in the subsequent sections.

3.1 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 personal identification number (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.

Deleted: [

Deleted:]

Deleted: Access Control

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 to provide consistent and secure means for performing the authentication function preceding an access control decision.

Deleted: access control

Deleted: discussed

Figure 3-1 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.

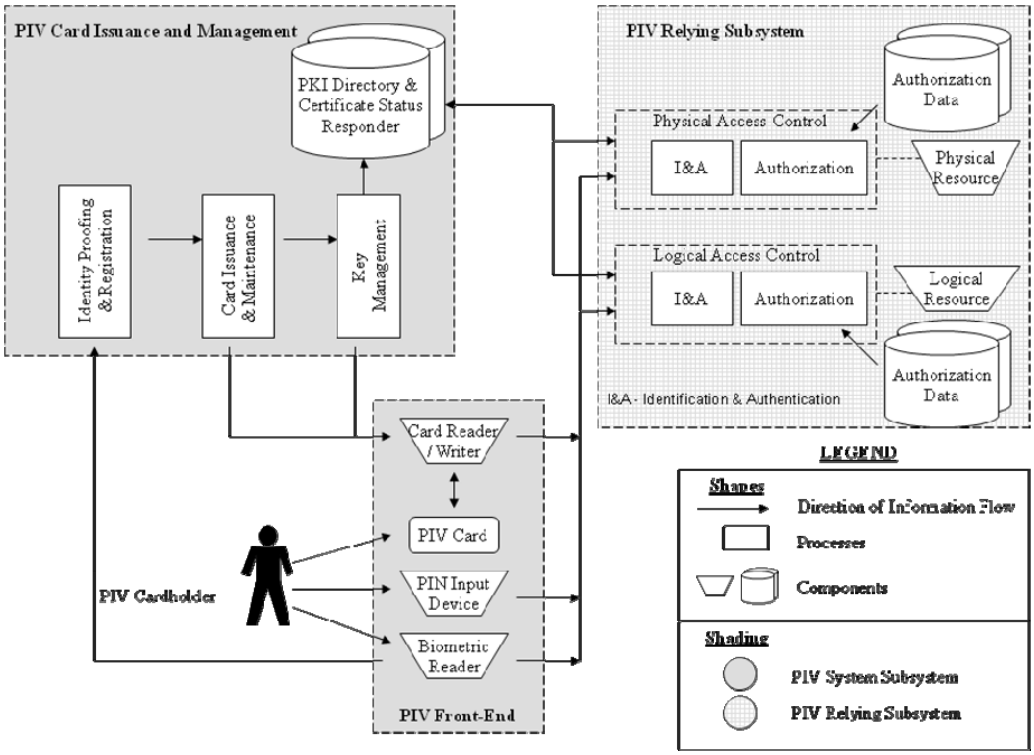


Figure 3-1. PIV System Notional Model

3.1.1 PIV Front-End Subsystem

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 that are very similar to the card readers personalize and initialize the information stored on PIV Cards. 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.

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 providing the card ("something you have").[5]

PIN input devices can also 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 introduces the use of an additional factor of authentication ("something you know") to control access to information resident on the card ("something you have"). This provides for a higher level of authentication assurance.

Deleted: (
Deleted:)
Deleted: (
Deleted:).

3.1.2 PIV Card Issuance and Management Subsystem

The identity proofing and registration component in Figure 3-1 refers to the process of collecting, storing, and maintaining all information and documentation that is 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.

Deleted: not only
Deleted: , but also
Deleted: A PIN is used to control the ability to unlock the card by the cardholder and then supply the embedded credentials for authentication purposes.

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 life cycle of PIV Cards—from generation and loading of authentication keys and PKI credentials, to usage of these keys for secure operations, to eventual renewal, 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.

Deleted: key

3.1.3 PIV Relying Subsystem

Deleted: Access Control

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.

Deleted: access control
Deleted: entrance
Deleted: turnstile,
Deleted: gate

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 to identify and authenticate cardholders. Once authenticated, the authorization component interacts with the authorization data component to match the cardholder-provided information to the information on record.

[5] For more information on the terms "something you know," "something you have," and "something you are," see [SP800-63].

The access control components typically interface with the card reader, the authorization component, the PIN input device, the biometric reader, and any certificate status service (if available).

Deleted: data

3.2 PIV Card Life Cycle Activities

The PIV Card life cycle 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 life cycle model. Figure 3-2 presents these PIV activities and depicts the PIV Card request as the initial activity and PIV Card termination as the end of life.

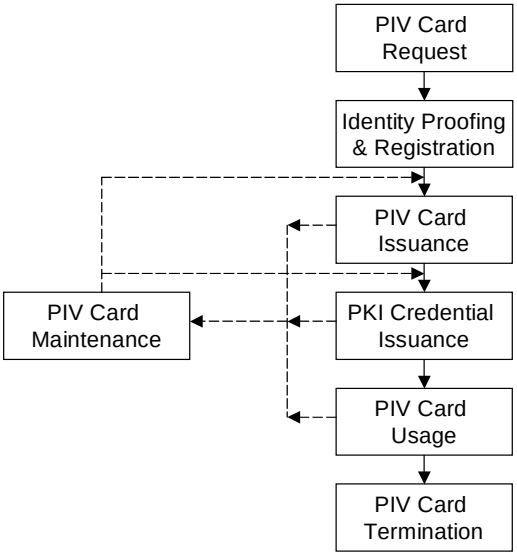


Figure 3-2. PIV Card Life Cycle Activities

Descriptions of the seven card life cycle 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 and that the entire set of identity source documents presented at the time of registration is valid.
- **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, PIN, 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.

Deleted: PIV

Deleted: PIV

4. PIV Front-End Subsystem

This section identifies the requirements for the components of the PIV front-end subsystem. Section 4.1 provides the physical and logical card specifications. The logical PIV Cardholder Unique Identifier (CHUID) object is described in Section 4.2. Cryptographic keys associated with the cardholder are described in Section 4.3. Formats for mandatory biometric information are defined in Section 4.4. Section 4.5 discusses card readers.

Deleted: reader specifications

Deleted: Topology

4.1 Physical PIV Card Characteristics

References to the PIV Card in this section and Sections 4.1.1 through 4.1.5 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.

Deleted: 4

Deleted: and physical topology

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.

Deleted: Sections 4.1.1 through 4.1.4 contain information related to the physical topology of the PIV Card.

Deleted: topology,

Deleted: ,

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].

4.1.1 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.

4.1.2 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
- Watermarks.

Incorporation of security features shall—

- Be in accordance with durability requirements [ISO7810]
- Be free of defects, such as fading and discoloration
- Not obscure printed information
- 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.

4.1.3 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. Only a security feature, as in Section 4.1.2, 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 reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a two percent soap solution.
- 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.
- Departments and agencies shall ensure that the card meets the requirements of Section 508 of the Rehabilitation Act. There are methods by which proper card orientation can be correctly detected by touch. One method is adherence of a raised surface (for example, an adhesive Braille letter). Section 4.1.4.3 defines Zone 21F, where raised surface may be placed.

Deleted: The PIV Card may be subjected to additional testing.¶

- 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 except as described in support of the Section 508 requirement.

- 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
  - 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.

Deleted: An alternative for allowing the card to be worn without physically altering it is through the use of various commercially available card holders and carriers. Card carriers are recommended in lieu of physically altering the card with an opening.¶

The PIV Card may be subjected to additional testing.

4.1.4 Visual Card Topography

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 4.1.6.

Deleted: 5

As noted in Section 4.1.3, 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).

Deleted: as do

Deleted: topology

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.

4.1.4.1 Mandatory Items on the Front of the PIV Card

Zone 1F—Photograph. The photograph shall be placed in the upper left corner, as depicted in Figure 4-1, and be a full frontal pose from top of the head to shoulder. A minimum of 300 dots per inch (dpi) resolution shall be used. The background should follow recommendations set forth in SP 800-76.

Zone 2F—Name. The full name[7] shall be printed directly under the photograph in capital letters. The full name shall be composed of a Primary Identifier (i.e., surnames or family names) and a Secondary Identifier (i.e., pre-names or given names). The full name shall be printed in the <Primary Identifier>, <Secondary Identifier> format. The entire full name should be printed on available lines of Zone 2F and either identifier could be wrapped. The wrapped identifier shall be indicated with ">" character at the end of the line. The identifiers may be confined to their lines if each fits on one line. Table 4-1 provides examples of separate Primary and Secondary Identifier lines, single line with identifiers, wrapped full names, and full name in three lines. Note that the truncation should only occur if the full name cannot be printed in 7 point font.

Deleted: *1*

Deleted: , as depicted in Figure 4-1

Deleted: *Zone 2—Name*. The full name

Deleted: [6] shall be printed directly under the photograph in capital letters. The font shall be a minimum of 10 point.¶ *Zone 8*

Table 4-1. Name Examples

Name: Anna Maria Eriksson Characteristics: simple full name, two lines sufficient with 10 points.	ERIKSSON, ANNA MARIA Ⓖ
Name: Anna Maria Eriksson Characteristics: simple full name, one line sufficient for full name with 10 points.	ERIKSSON, ANNA MARIA Ⓖ
Name: Susie Margaret Smith-Jones Characteristics: longer full name in two lines, sufficient space in 10 points.	SMITH-JONES, SUSIE MARGARET Ⓖ
Name: Susie Margaret Smith-Jones Characteristics: longer full name wrapped, two lines sufficient with 10 points.	SMITH-JONES, SUSIE MA> RGARET Ⓖ
Name: Chayapa Dejthamrong Krusuang Nilavadhanananda Characteristics: longer full name wrapped, two lines NOT sufficient with 10 points. Reduce the font size to 8 points.	NILAVADHANANANDA, CHAYA> PA DEJTHAMRONG KRUSUANG Ⓖ

[7] Alternatively, pseudonyms as provided under the law as discussed in Section 2.6.4.

Name: Vaasa Silvaan Bennelong Wooloomooloo Warrandyte Warnambool Characteristics: longer full name, two lines NOT sufficient with 8 point, 7 point allows sufficient space for three lines in Zone 2F.	BEENELONG WOOLOOMOOLOO WARRANDYTE WARWARNAMBOOL, VAASA SILVAAN G
Name: Vaasa Silvaan Bennelong Wooloomooloo Warrandyte Warnambool Characteristics: same as previous but full name is wrapped.	BEENELONG WOOLOOMOOLOO W> ARRANDYTE WARWARNAMBOOL, V> AASA SILVAAN G

Names in the Primary Identifier and the first name in the Secondary Identifier shall not be abbreviated. Other names and conventional prefixes and suffixes may be abbreviated. The special character "." (period) shall indicate such abbreviations, as shown in Figure 4-2. Other uses of special symbols (e.g., "O'BRIEN") are at the discretion of the issuer.

Departments and agencies shall use the largest font size of 8 to 10 points that allows the full name to be printed. The font size 7 point allows space for 3 lines and shall only be used if the full name is greater than 45 characters.

Zone 8F—Employee Affiliation. An employee affiliation shall be printed on the card. Some examples of employee affiliation are "Employee", "Contractor," "Active Duty," and "Civilian."

Zone 10F—Agency, Department, or Organization. The Organizational Affiliation shall be printed as depicted in Figure 4-1.

Zone 14F—Expiration Date. The card expiration date shall be printed in a YYYYMMMDD format.

Deleted: A printed

Deleted: *Zone 10— Organizational Affiliation*

Deleted: *14*

4.1.4.2 Mandatory Items on the Back of the Card

Zone 1B—Agency Card Serial Number. This item shall be printed as depicted in Figure 4-6 and contain the unique serial number from the issuing department or agency. The format shall be at the discretion of the issuing department or agency.

Zone 2B—Issuer Identification Number. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code and four characters for the agency code that uniquely identifies the department or agency.

Deleted: *1*

Deleted: (see an important at the end of this document)

Deleted: *2*

Deleted: (see an important at the end of this document)

Deleted: ,

Deleted: , and a five-digit number

Deleted: issuing facility within the

4.1.4.3 Optional Items on the Front of the Card

This section contains a description of the optional information and machine-readable technologies that may be used and their respective placement. The storage capacity of all optional technologies is as prescribed by individual departments and agencies and is not addressed in this standard. Although the items discussed in this section are optional, if used they shall be placed on the card as designated in the examples provided and as noted.

Zone 3F—Signature. If used, the department or agency shall place the cardholder signature below the photograph and cardholder name as depicted in Figure 4-3. The space for the signature shall not interfere with the contact and contactless placement. Because of card surface space constraints, placement of a signature may limit the size of the optional two-dimensional bar code.

Zone 4F—Agency Specific Text Area. If used, this area can be used for printing agency specific requirements, such as employee status.

Zone 5F—Rank. If used, the cardholder's rank shall be printed in the area as illustrated. Data format is at the department or agency's discretion.

Zone 6F—Portable Data File (PDF) Two-Dimensional Bar Code. If used, the PDF bar code placement shall be as depicted in Figure 4-2 (i.e., left side of the card). If Zone 3F (a cardholder signature) is used, the size of the PDF bar code may be affected. The card issuer should confirm that a PDF used in conjunction with a PIV Card containing a cardholder signature will satisfy the anticipated PDF data storage requirements.

Zone 9F— Header. If used, the text *"United States Government"* shall be placed as depicted in Figure 4-1. Departments and agencies may also choose to use this zone for other department or agency-specific information, such as identifying a Federal emergency responder role, as depicted in Figure 4-2.

Zone 11F—Agency Seal. If used, the seal selected by the issuing department, agency, or organization shall be printed in the area depicted. It shall be printed using the guidelines provided in Figure 4-2 to ensure information printed on the seal is legible and clearly visible.

Zone 12F—Footer. The footer is the preferred location for the *Emergency Response Official Identification* label. If used, a department or agency may print "Emergency Response Official" as depicted in Figure 4-2, preferably in white lettering on a red background. Departments and agencies may also use Zone 9F to further identify the Federal emergency respondent's official role. Some examples of official roles are "Law Enforcement", "Fire Fighter", and "Emergency Response Team (ERT)".

Zone 13F—Issue Date. If used, the card issuance date shall be printed above the expiration date in YYYYMMMDD format as depicted in Figure 4-2.

Zone 15F—Color-Coding for Employee Affiliation. Color-coding may be used for additional identification of employee affiliation (see Section 4.1.5 for Color Representation). If color-coding is used, it shall be used as a background color for Zone 2F (name) as depicted in Figure 4-4. The following color scheme shall be used for the noted categories:

+ Blue—foreign nationals
+ Red—emergency response officials
+ Green—contractors.

These colors shall be reserved and shall not be employed for other purposes. Also, these colors shall be printed in accordance to the color specifications provided in Section 4.1.5. Zone 15F may be a solid or patterned line at the department or agency's discretion.

Zone 16F—Photo Border for Employee Affiliation. A border may be used with the photo to further identify employee affiliation, as depicted in Figure 4-3. This border may be used in conjunction with

Deleted: 3
Deleted: topology
Deleted: 4
Deleted: 5
Deleted: 6
Deleted: the diagram
Deleted: 3
Deleted: 9
Deleted: 11
Deleted: 12
Deleted: Federal
Deleted: text
Deleted: print a secondary line in
Deleted: 9
Deleted: , "Firefighter"
Deleted: 13
Deleted: 15
Deleted: .
Deleted: 2
Deleted: responder
Deleted: Zone 15
Deleted: 16

Zone 15F to enable departments and agencies to develop various employee categories. The photo border shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the department or agency's discretion.

Zone 17F—Agency Specific Data. In cases in which other defined optional elements are not used, Zone 17F may be used for other department or agency-specific information, as depicted in Figure 4-5.

Zone 18F—Affiliation Color Code. The affiliation color code "B" for Blue, "G" for Green, or "R" for Red shall be printed in a white circle in Zone 15F. The diameter of the circle shall not be more than 5 mm. Note that the lettering shall correspond to the printed color in Zone 15F. If Zone 16F photo border coloring is used to identify employee affiliation of emergency response officials, foreign nationals, or contractors, the lettering shall correspond to the printed color.

Zone 19F—Expiration Date. If used, the card expiration date shall be printed in a MMMYYYY format in the upper right hand corner. The Zone 19F expiration date shall be printed in Arial 12pt Bold.

Zone 20F—Organizational Affiliation Abbreviation. The organizational affiliation abbreviation may be printed in the upper right hand corner below the Zone 19F expiration date as shown in Figure 4-1. If printed, the organizational affiliation abbreviation shall be printed in Arial 12pt Bold.

Zone 21F—Section 508 Compliance. A raised surface may be created so a card orientation can be determined by touch. The thickness of the PIV Card after the raised surface is applied shall not exceed 54 mil. See Figure 4-2 for the placement of the raised surface.

4.1.4.4 Optional Items on the Back of the Card

Zone 3B—Magnetic Stripe. If used, the magnetic stripe shall be high coercivity and placed in accordance with [ISO7811], as illustrated in Figure 4-7.

Zone 4B—Return Address. If used, the "return if lost" language shall be generally placed on the back of the card as depicted in Figure 4-7.

Zone 5B—Physical Characteristics of Cardholder. If used, the cardholder physical characteristics (e.g., height, eye color, hair color) shall be printed in the general area illustrated in Figure 4-7. Additional information such as Gender and Date of Birth required for Transportation Security Administration (TSA) checkpoint may also be printed as shown in Figure 4-7.

Zone 6B—Additional Language for Emergency Response Officials. Departments and agencies may choose to provide additional information to identify emergency response officials or to better identify the cardholder's authorized access. If used, this additional text shall be in the general area depicted and shall not interfere with other printed text or machine-readable components. An example of a printed statement is provided in Figure 4-7.

Zone 7B—Standard Section 499, Title 18 Language. If used, standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the card shall be printed in the general area depicted in Figure 4-7.

Zone 8B—Linear 3 of 9 Bar Code. If used, a linear 3 of 9 bar code shall be generally placed as depicted in Figure 4-7. It shall be in accordance with Association for Automatic Identification and Mobility (AIM) standards. Beginning and end points of the bar code will be dependent on the embedded contactless

Deleted: 15
Deleted: 17
Deleted: 17
Deleted: 3
Deleted: 4
Deleted: To
Deleted: 5
Deleted: 6
Deleted: Responder
Deleted: 7
Deleted: 8

module selected. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.

Zone 9B—Agency-Specific Text. In cases in which other defined optional elements are not used, Zone 9B may be used for other department or agency-specific information, as depicted in Figure 4-8. For example, emergency response officials may use this area to provide additional details.

Zone 10B—Agency-Specific Text. Zone 10B is similar to Zone 9B in that it is another area for providing department or agency-specific information.

For Zones 9B and 10B, departments and agencies are encouraged to use this area prudently and minimize printed text to that which is absolutely necessary.

In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by the Geneva Accord and to facilitate legislatively mandated medical entitlements.

Deleted: *9*

Deleted: 9

Deleted: **(s**ee an important at the end of this document**)**.

Deleted: responder

Deleted: *10*

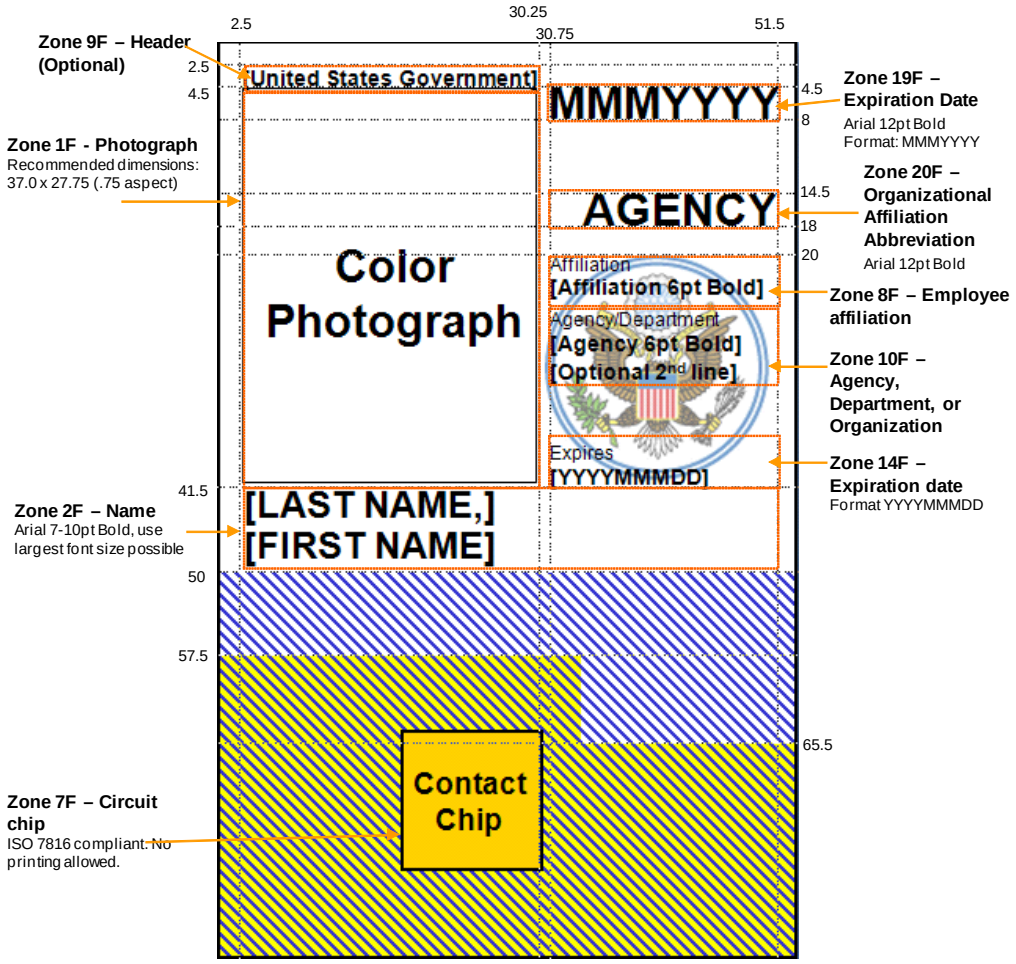
Deleted: 10

Deleted: 9

Deleted: 9

Deleted: 10

Deleted: medical entitlements that are



Area for additional optional data. Agency-specific data may be printed in this area. See other examples for required placement of additional optional data elements.

Area likely to be needed by card manufacturer. Optional data may be printed in this area but may be subject to restrictions imposed by card and/or printer manufacturers.

Figure 4-1. Card Front—Printable Areas

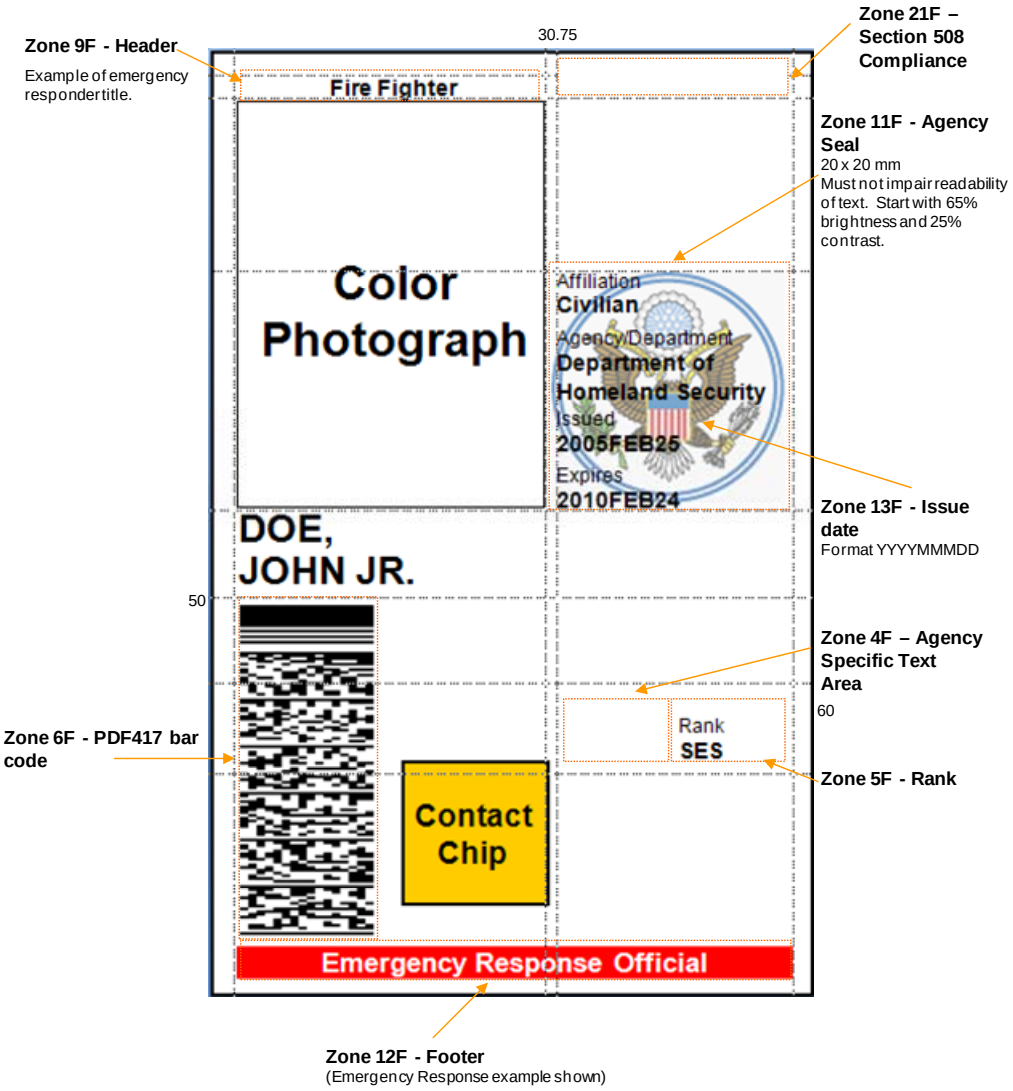


Figure 4-2. Card Front—Optional Data Placement—Example 1

All measurements around the figure are in millimeters and are from the top left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

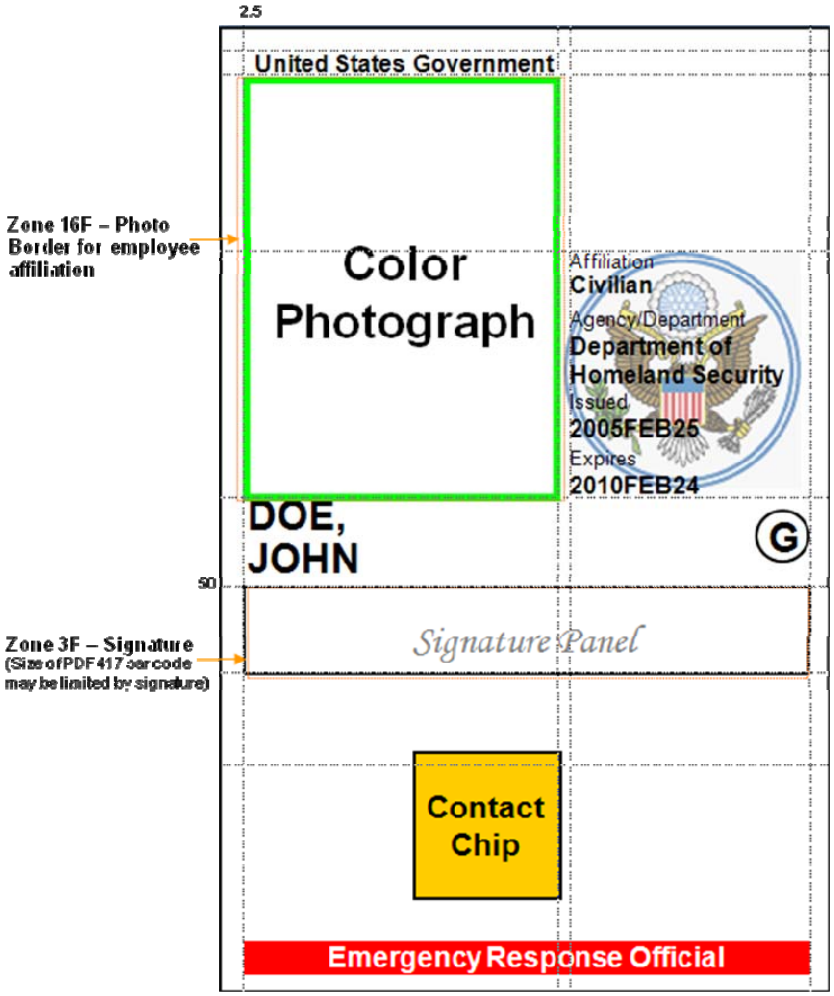


Figure 4-3. Card Front—Optional Data Placement—Example 2

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

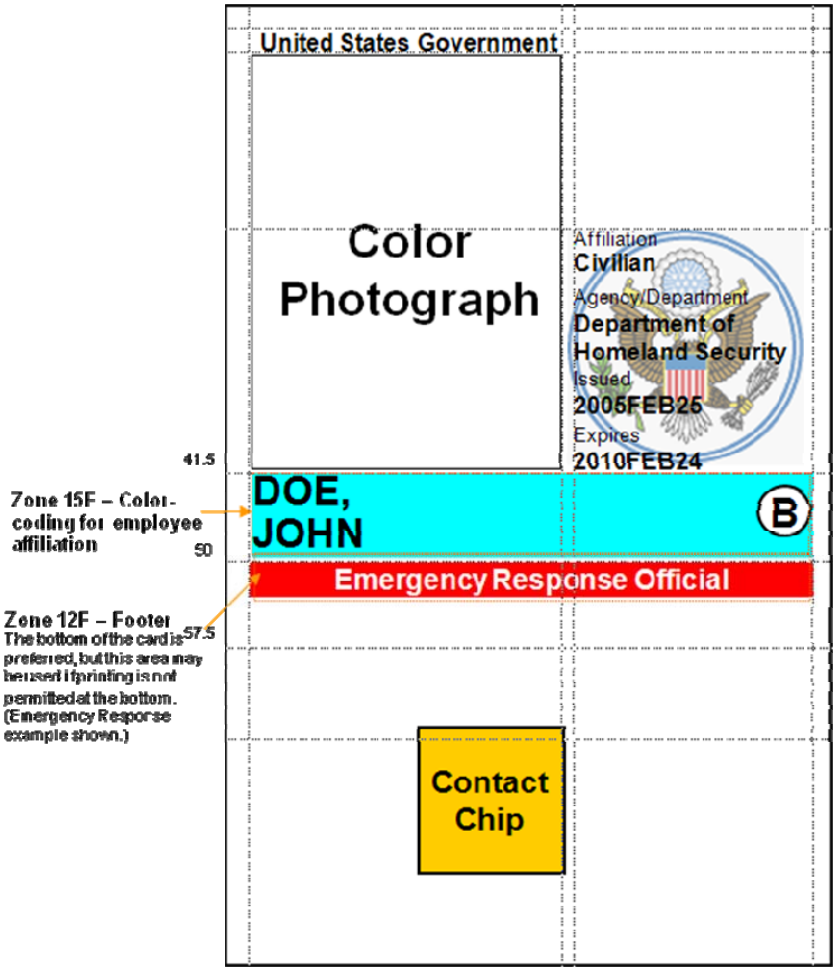


Figure 4-4. Card Front—Optional Data Placement—Example 3

All measurements around the figure are in millimeters and are from the top-left corner.
All text is to be printed using the Arial font.
Unless otherwise specified, the font size should be 5pt normal weight for tags and 6pt bold for data.

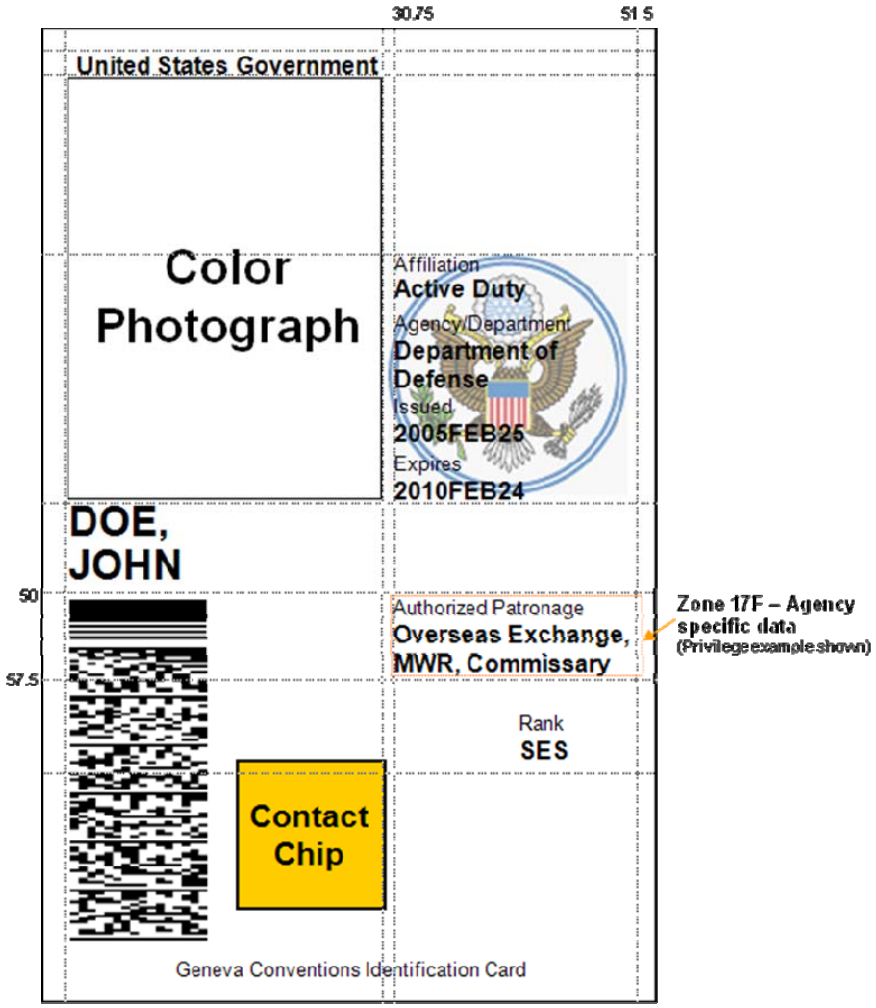


Figure 4-5. Card Front—Optional Data Placement—Example 4

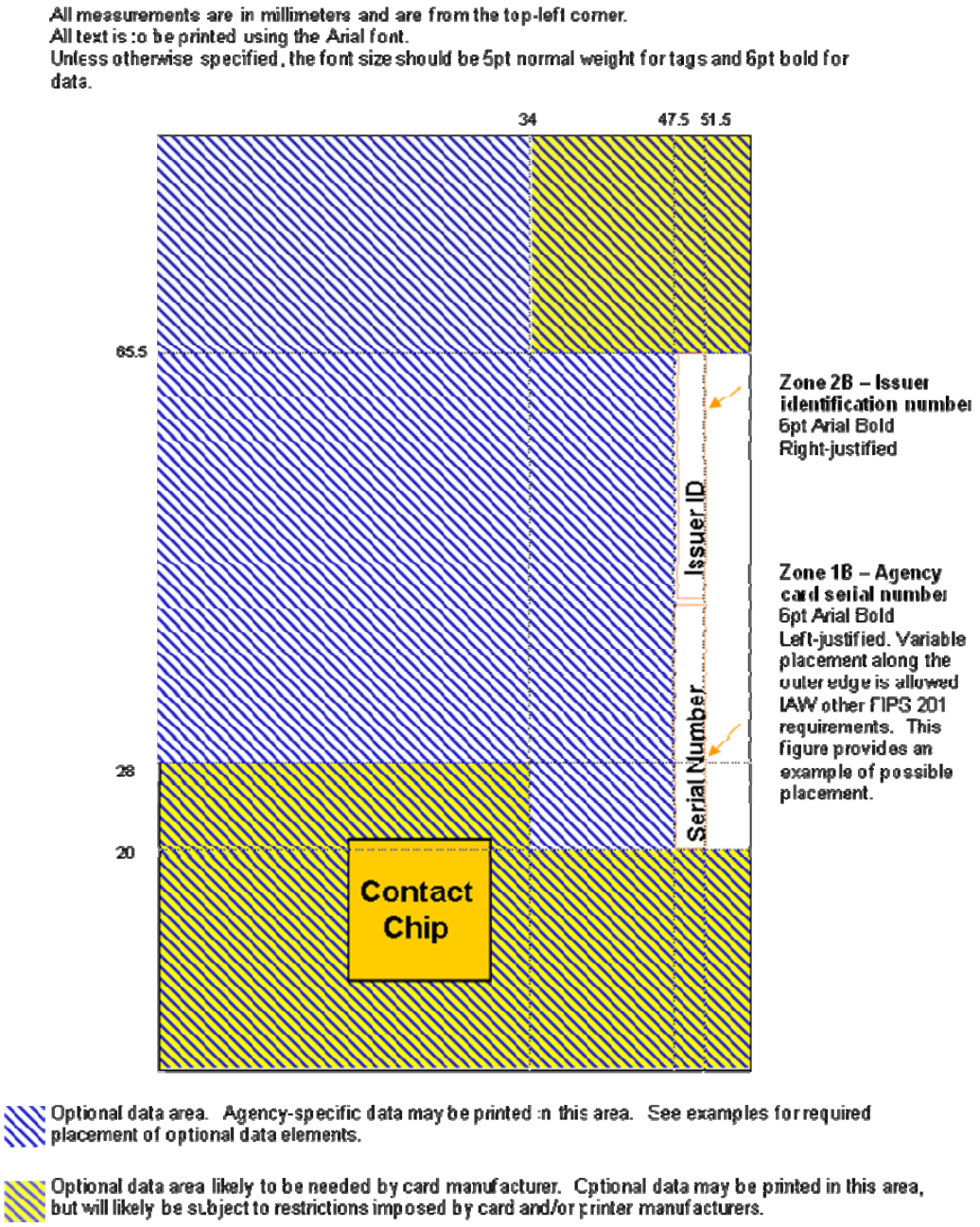


Figure 4-6. Card Back—Printable Areas and Required Data

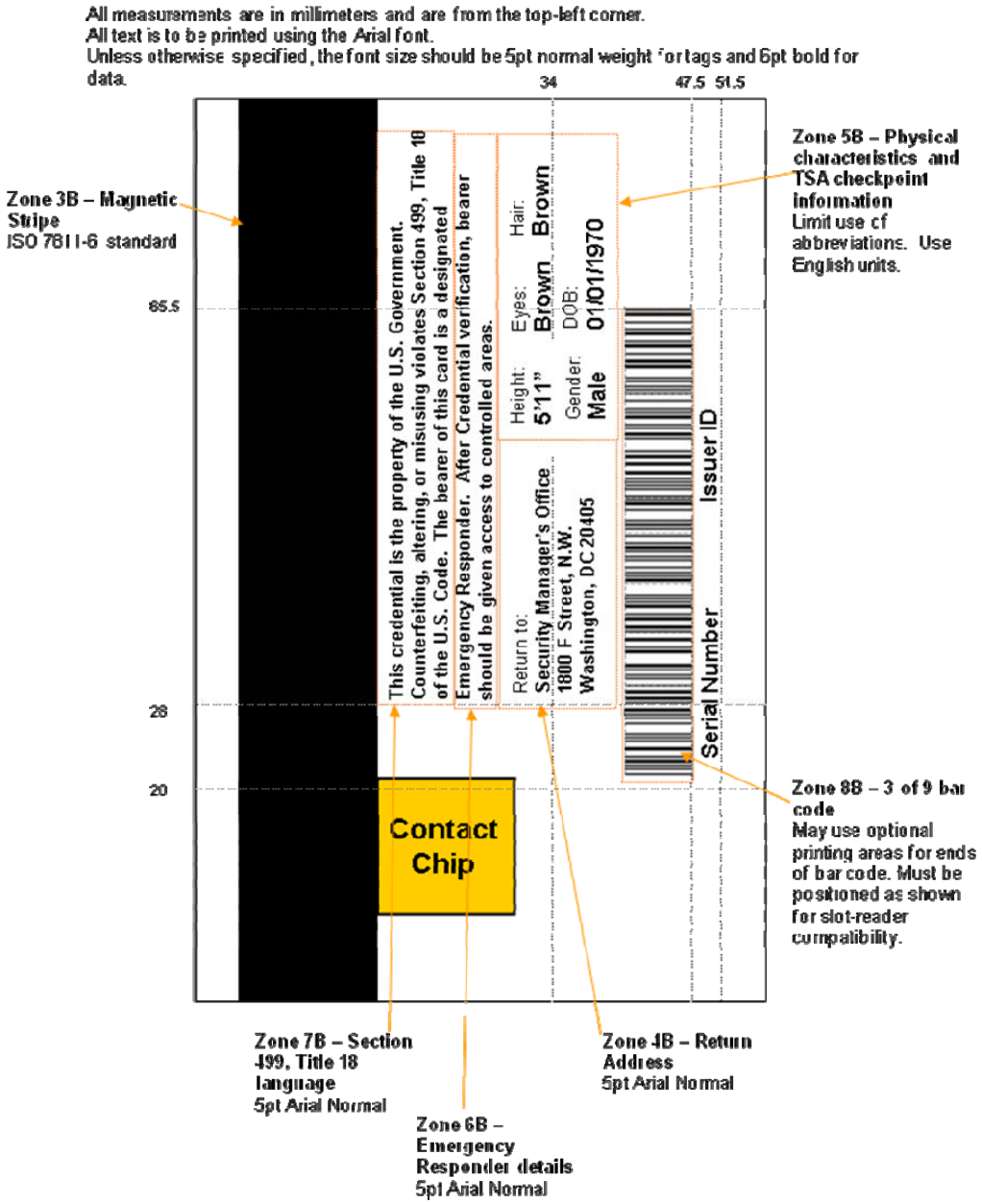


Figure 4-7. Card Back—Optional Data Placement—Example 1

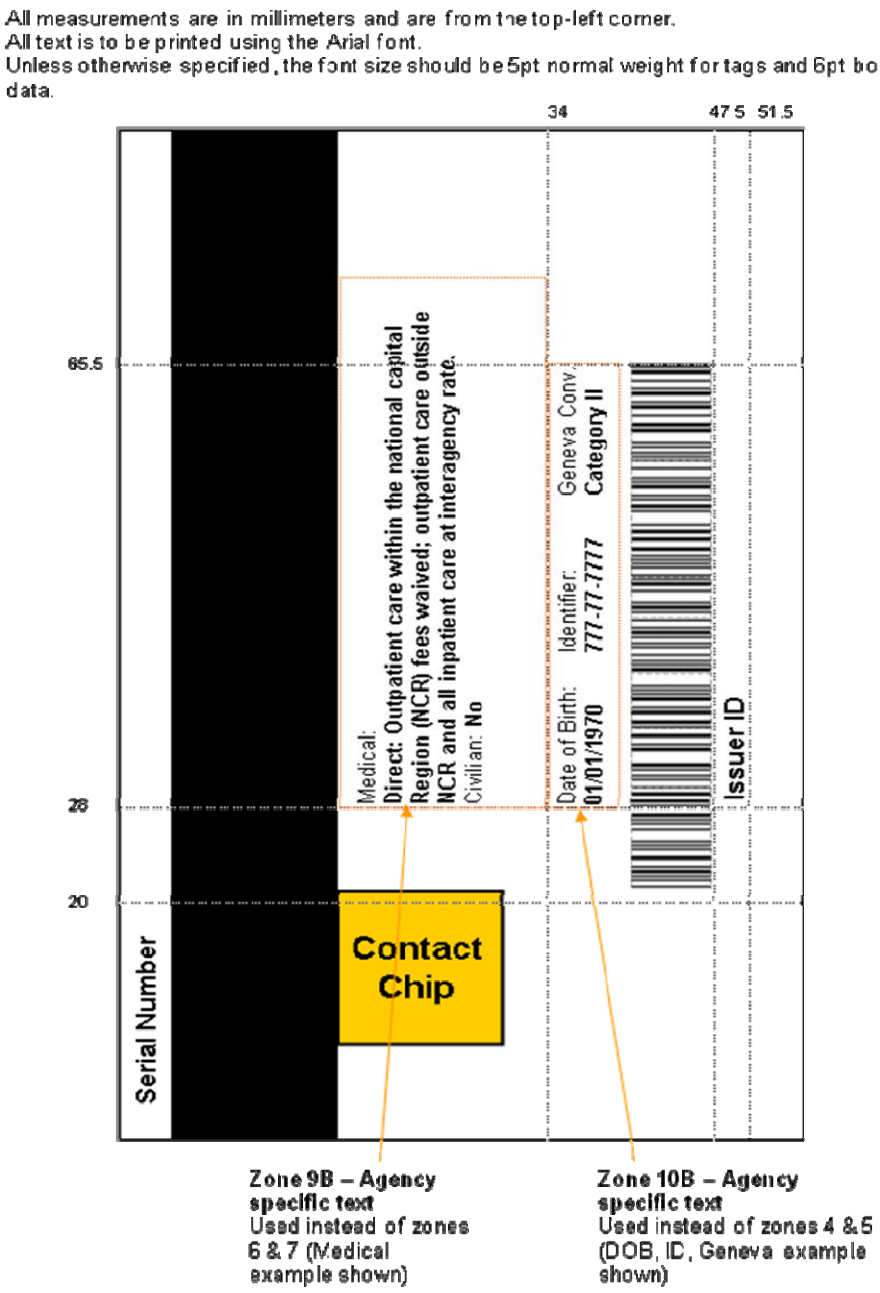


Figure 4-8. Card Back—Optional Data Placement—Example 2

4.1.5 Color Representation

Table 4-1 provides quantitative specifications for colors in three different color systems: sRGB Tristimulus, sRGB ([IEC 61966], Color management – default RGB color space), and CMYK (Cyan, Magenta, Yellow and Key or 'blacK'). Since the card body is white, the white color-coding is achieved by the absence of printing. Note that presence of the security feature, which may overlap colored or printed regions, may modify the perceived color. In the case of colored regions, the effect of overlap shall not prevent the recognition of the principal color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.

Table 4-2. Color Representation

Color	Zone	sRGB Tristimulus Value (IEC 61966-2-1)	sRGB Value (IEC 61966-2-1)	CMYK Value {C,M,Y,K}
White	15F	{255, 255, 255}	{255, 255, 255}	{0, 0, 0, 0}
Green	15F	{153, 255, 153}	{203, 255, 203}	{40, 0, 40, 0}
Blue	15F	{0, 255, 255}	{0, 255, 255}	{100, 0, 0, 0}
Red	12F	{253, 27, 20}	{254, 92, 79}	{0, 90, 86, 0}

The colors in Table 4-2 can be mapped to the Pantone[8] color cue; however, note that this will not produce an exact match. An agency or department may use the following Pantone mappings in cases where Table 4-2 scales are not available.

- Blue—630C
- White—White
- Green—359C
- Red—032C

4.1.6 Logical Credentials

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

Deleted: Specifically, it provides details of the composition of an identity credential and its activation.

4.1.6.1 Logical Credential Data Model

To support a variety of authentication mechanisms, the PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements are part of the data model for PIV logical credentials, and include the following:

Deleted: collectively comprise

- A PIN
- A CHUID
- PIV authentication data (one asymmetric key pair and corresponding certificate)
- Two biometric fingerprints or if fingerprints are not collectible, two iris images

Deleted: .

[8] Pantone is a registered name protected by law.

- Card authentication data (one asymmetric key pair and corresponding certificate)

This standard also defines optional data elements for the PIV data model. These optional data elements include:

- An asymmetric key pair and corresponding certificate for digital signatures
- An asymmetric key pair and corresponding certificate for key management
- A symmetric card authentication key for supporting physical access applications
- A symmetric key associated with the card management system.
- Facial image
- One or two iris images
- On-card biometric comparison data

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)
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 card management key into the second category, and the CHUID, biometric credential, symmetric keys, and asymmetric keys into the third.

4.1.7 PIV Card Activation

The PIV Card shall be activated[9] to perform privileged[10] operations such as reading biometric information and using the PIV authentication key, digital signature key, and key management key. The PIV Card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system. Cardholder activation is described in Section 4.1.7.1, and card management system activation is described in Section 4.1.7.2.

4.1.7.1 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, 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

[9] Activation in this context refers to the unlocking of the PIV Card application so privileged operations can be performed.
[10] A read of a PIV CHUID or use of the card authentication key is not considered a privileged operation.

Deleted: The PIV data model may be optionally extended to meet department or agency-specific requirements. If the data model is extended, this standard establishes requirements for the following four classes of logical credentials:¶

Deleted: Asymmetric or
Deleted: keys
Deleted: additional
Deleted: (s)

Deleted: PINs fall
Deleted: keys
Deleted: information

Deleted: must
Deleted: asymmetric keys

Deleted: authentication
Deleted: 6
Deleted: authentication
Deleted: 6

Deleted: PIN

Deleted: PIN

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 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.

4.1.7.2 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, card management keys shall be set to be specific to each PIV Card. That is, each PIV Card shall contain a unique card management key. Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP 800-78]

Deleted: presented PIN

Deleted: correct

Deleted: limit the

Deleted: guesses an adversary can attempt if a card is lost or stolen. Moreover,

Deleted: authentication mechanism

Deleted: meet the identity-based authentication requirements

Deleted: FIPS PUB 140-2 Level 2. [FIPS140-2]

Deleted: SP800

Deleted: SP800

4.2 Cardholder Unique Identifier (CHUID)

The PIV Card shall include the CHUID as defined in [SP 800-73]. The CHUID includes the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card as described in [SP 800-73]. CHUID elements specific to this standard are described below in Section 4.2.1. The format of the CHUID signature element is described in Section 4.2.2.

The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation. The PIV FASC-N shall not be modified post-issuance.

The CHUID may be read and used by the relying systems, but it should be treated as if it were a password (since the digital signature provides entropy equivalent to a password) for purposes of retention. A stored CHUID presents risks similar to a stored password; it can be copied and used to gain access. It is strongly recommended that a complete CHUID should not be stored in relying systems.

Deleted: The PACS Implementation Guidance [PACS] defines the CHUID data object; this description is refined in [SP800-73].

Deleted: SP800

Deleted: an element,

Deleted: .

4.2.1 PIV CHUID Data Elements

In addition to the mandatory FASC-N that identifies a PIV Card, the CHUID shall include an expiration date data element in machine readable format that specifies when the card expires. The expiration date format and encoding rules are as specified in [SP 800-73]. For PIV Cards, the format of the asymmetric signature field is specified in Section 4.2.2.

Deleted: .

Deleted: , the expiration date data element shall specify

Deleted: SP800

4.2.2 Asymmetric Signature Field in CHUID

This standard requires inclusion of the asymmetric signature field in the CHUID container. The asymmetric signature data element of the PIV CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as defined in RFC 5652 [RFC5652]. The digital signature shall be computed in accordance with [SP 800-73]. Algorithm and key size requirements for the asymmetric signature are detailed in [SP 800-78].

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

- The message shall include a *version* field specifying version v3

Deleted: 3852 [RFC3852

Deleted: over the entire contents of the CHUID, excluding the Asymmetric Signature field.

Deleted: SP800

Deleted: RFC3852

- The *digestAlgorithms* field shall be as specified in [SP 800-78]
- The *encapContentInfo* shall:
  - Specify an *eContentType* of id-PIV-CHUIDSecurityObject
  - Omit the *eContent* field
- The *certificates* field shall include only a single X.509 certificate, which can be used to verify the signature in the *SignerInfo* field
- The *crls* field shall be omitted
- *signerInfo*s shall be present and include only a single *SignerInfo*
- The *SignerInfo* shall:
  - Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
  - Specify a *digestAlgorithm* in accordance with [SP 800-78]
  - Include, at a minimum, the following signed attributes:
    - A *MessageDigest* attribute containing the hash computed in accordance with [SP 800-73]
    - A *pivSigner-DN* attribute containing the subject name that appears in the PKI certificate for the entity that signed the CHUID
  - Include the digital signature.

The public key required to verify the digital signature shall be provided in the *certificates* field in an X.509 digital signature certificate issued under the id-fpki-common-devices, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON].[11] The X.509 digital signature certificate issued under the id-fpki-common-devices, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON] shall also include an extended key usage (*extKeyUsage*) extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix D.

4.3 Cryptographic Specifications

The PIV Card shall implement the cryptographic operations and support functions as defined in [SP 800-78] and [SP 800-73].

The PIV Card must store private keys and corresponding public key certificates, and perform cryptographic operations using the asymmetric private keys. 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*. With the exception of the *card authentication key and keys used to establish a secure messaging*, the cryptographic private key operations shall be performed only through the contact interface.

[11] For legacy PKIs, as defined in Section 5.4, the certificates may be issued under a department or agency-specific policy that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

Deleted: SP800

Deleted: SP800

Deleted: over the concatenated contents of the CHUID, excluding the asymmetric signature field

Deleted:], and shall meet the format and infrastructure requirements for PIV

Deleted: keys specified in Section 4.3. The

Deleted: *extendedKeyUsage*

Deleted: At a minimum,

Deleted: one asymmetric

Deleted: key

Deleted: a

Deleted: certificate

Deleted: key. Cryptographic operations with this

Deleted: are

The PIV Card may include additional asymmetric keys and PKI certificates. This standard defines requirements for digital signature and key management keys. Where digital signature keys are supported, the PIV Card is not required to implement a secure hash algorithm. Message hashing may be performed off card. 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].

The PIV Card has both mandatory keys and optional keys:

- The *PIV authentication key* shall be an asymmetric private key that is accessible from the contact interface and supports card authentication for an interoperable environment. This is a mandatory key for each PIV Card.
- The *asymmetric card authentication key* shall be a private key that is accessible over the contactless and contact interface and supports card authentication for an interoperable environment. This is a mandatory key for each PIV Card.
- The *symmetric (secret) card authentication key* supports card authentication for physical access, and it is optional.
- The *digital signature key* is an asymmetric private key supporting document signing, and it is optional.
- 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. Optionally, up to twenty retired key management keys may also be stored on the PIV Card.
- The *card management key* is a symmetric key used for personalization and post-issuance activities, and it is optional.
- The PIV Card may include additional key(s) for use with secure messaging to enable protocols such as on-card biometric comparison. These keys are defined in [SP 800-73] or [SP 800-78].

All PIV cryptographic keys shall be generated within a FIPS 140 validated cryptographic module with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage.

Requirements specific to storage and access for each key are detailed below. Where applicable, key management requirements are also specified.

- **PIV Authentication Key.** This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV authentication key. The PIV authentication key must be available only through the contact interface 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).

Deleted: The PIV Card shall implement 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.¶

Deleted: -

Deleted: If the contactless interface utilizes asymmetric cryptography (e.g., elliptic curve cryptography [ECC]), the PIV Card may also require storage for a corresponding public key certificate.

Deleted: All cryptographic operations using the PIV keys shall be performed on-card; 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].¶

Deleted: a single

Deleted: key

Deleted: four types of

Deleted: supporting

Deleted: , and it

Deleted: may be either a symmetric (secret) key or an asymmetric private key for

Deleted: -2

Deleted: cryptomodule

Deleted: of

Deleted: class of keys

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Issued PIV Authentication certificates shall also include a PIV NACI indicator extension until such time that OMB approves a government-wide operational system for distribution of Background Investigation status information (see Section 2.5). After OMB approves such an operational system, the inclusion of the PIV NACI indicator extension in issued PIV Authentication certificates is optional and deprecated. Section 5 of this document specifies the certificate format and the key management infrastructure for PIV authentication key.

+ **Asymmetric Card Authentication Key.** The asymmetric card authentication key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the card authentication key. The card authentication key shall be available through the contact and the contactless interface 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).

  The PIV Card shall store a corresponding X.509 certificate to support validation of the asymmetric card authentication key. The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for asymmetric PIV Card authentication keys.

+ **Symmetric Card Authentication Key.** The symmetric card authentication key is imported onto the card by the issuer. The PIV Card shall not permit exportation of this key. 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 card authentication key shall be available through the contact and the contactless interface of the PIV Card. This standard does not specify key management protocols or infrastructure requirements.

+ **Digital Signature Key.** 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 interface of the PIV Card. Private key operations may not be performed without explicit user action.

  The PIV Card shall store a corresponding X.509 certificate to support validation of the digital signature key. Section 5 of this document specifies the certificate format and the key management infrastructure for PIV digital signature keys.

+ **Key Management Key.** This key may be generated on the PIV Card or imported to the card. If present, the key management key must only be accessible using the contact interface 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).

  The PIV Card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5 of this document specifies the certificate format and the key management infrastructure for key management keys.

Deleted: The

Deleted: certificate

Deleted: ; this non-critical private extension indicates the

Deleted: of the subject's background investigation at the time of card issuance.

Deleted: .4

Deleted: keys

Deleted: /secret

Deleted: explicit user action

Deleted:).

Deleted: .4

Deleted: This key is sometimes called an encryption key or an encipherment key.

Deleted: .4

Deleted: PIV

- **Card Management Key.** 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 of the PIV Card.

4.4 PIV Biometric Data Specifications

The PIV biometric data shall consist 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 and for performing visual authentication during card usage. The facial image is not required to be stored on the card.
- Two electronic fingerprints to be stored on the card for automated authentication during card usage. If no fingerprints can be collected, two electronic iris images shall be stored on the PIV Card.

The PIV biometric data may optionally include:

- One or two iris images
- On-card biometric comparison data

All biometric data enumerated above are collected during the identity proofing and registration process. PIV biometric data shall be stored on PIV Cards as specified in [SP 800-76] and [SP 800-73].

The PIV biometric data, except for on-card biometric comparison data, stored on the card shall be only accessible through the contact interface and after the presentation of a valid PIN. No contactless access is permitted for the PIV biometric data, except for on-card biometric comparison data, specified to be stored on the PIV Card under this standard. The on-card biometric comparison data may be available through the contact and the contactless interface of the PIV Card to support card activation (section 4.1.7.1) and cardholder authentication (section 6.2.5). The PIV Card shall not permit exportation of the on-card biometric comparison data. If implemented, PIV on-card biometric comparison data shall be implemented and used in accordance with [SP 800-73] and [SP 800-76].

4.4.1 Biometric Data Collection and chain-of-trust

A card issuer shall 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, and shall be 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[12]. An enrollment data record shall describe the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition method. An enrollment data record may or may not contain historical biometric data[13]. A card issuer shall retain a biometric record, for example two

[12] For example, ten fingerprints for law enforcement checks may be collected at one time and place, and two fingerprints for PIV Card templates may be collected at a later time and different place, provided that the two fingerprints are verified as among the ten original fingerprints.

[13] An enrollment data set will always include biometric data immediately after it is created, but the biometric data itself may be deleted from the enrollment data set when it is no longer needed. The most recent biometric data shall be retained in the chain of trust. This enables extending and reconnecting the chain of trust.

Deleted: See Section 4.1.6.2 for further details.

Deleted: 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 shall require explicit cardholder action, in addition to activation of the card.¶

Deleted: used during the PIV Card life cycle activities

Deleted: as well as

Deleted: A new facial image must be collected at the time of reissuance.

Deleted: three

Deleted: Implementation requirements for storage of

Deleted: is dependent on use of specifications contained

Deleted: NIST

Deleted: [SP800-76].

Deleted: The two electronic fingerprints

Deleted: only over

Deleted: , Storage,

Deleted: Usage

Deleted: The full set of fingerprints shall be 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].

fingerprint templates, from the most recent enrollment to extend the chain-of-trust when necessary.[14] If the card issuer cannot collect and retain two fingerprints templates, two iris images shall be retained as the biometric data for the chain-of-trust and used in 1:1 biometric match to reconnect to the chain-of-trust. The biometric data in the chain-of-trust shall be valid for at most 12 years.

A card issuer shall be able to import and export a chain-of-trust in the manner and representation described in [TBD].

The chain-of-trust will be applied in several situations to include:

+ Extended enrollment: a PIV applicant enrolls ten fingerprints for background investigations at one place and time (e.g., at a police station), and two fingerprints for on-card templates at another place and time (e.g., at the PIV enrollment station). The chain-of-trust would contain identifiers and two enrollment data records, one with a ten fingerprint transaction, and one with two fingerprint templates. The two fingerprint templates would be matched against the corresponding fingers in the ten fingerprint data set to link the chain.

+ Reissuance: a PIV cardholder loses his/her card. Since the card issuer has biometric enrollment data records, the cardholder can perform a 1:1 biometric match to reconnect to the card issuer's chain-of-trust. The card issuer need not repeat the background investigation. The card issuer proceeds to issue a new card as described in Section 2.5.2.

+ Interagency transfer: a Federal employee is transferred from one agency to another. When the employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the employee arrives at new agency and is processed in, the card issuer in the new agency requests the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction proceeds as a PIV Card Reissuance as described in Section 2.5.2.

The technical specifications for the collection and formatting of the ten fingerprints and other biometric information are contained in [SP 800-76]. The fingerprints shall be 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 [NISTIR7123]. Because biometric identification using fingerprints is the primary means for law enforcement checks, agencies shall seek OPM guidance for alternative means for performing law enforcement checks in cases where obtaining ten fingerprints is impossible.

In cases where the collection of fingerprints for the PIV Card is not possible, two iris images shall be collected from the PIV applicant. The technical specifications for the electronic iris images are contained in [SP 800-76]. The electronic iris images may be used for biometric authentication as defined in Section 6.2.3. This approach is required when the PIV Card does not contain fingerprint templates because the card issuer could not collect usable fingerprint images from the cardholder.

A facial image shall be collected from all PIV applicants. The technical specifications for an electronic facial image are contained in [SP 800-76]. The electronic facial image may be used for the following purposes:

Deleted: SP800

[14] If an agency is unable to collect fingerprint biometric data or iris images biometric data, a circumstance requiring PIV Card reissuance would force a new chain-of-trust to be created, implying a new FBI National Criminal History Check.

- For generating the printed image on the card
- For generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.1. This approach may be required in the following situations:
  - A good live sample of fingerprints or iris cannot be collected from the PIV cardholder due to damage or injury.
  - Fingerprint or iris matching equipment failure
  - Authenticating PIV cardholders covered under Section 508.

Two electronic fingerprints shall be 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 [SP 800-76]. The right and left index fingers shall normally be designated as the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary and secondary designations shall be 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

These fingerprint templates shall be used for 1:1 biometric verification against live samples collected from the PIV cardholder (see Section 6.2.3). 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 shall be used first. In cases where there is difficulty in collecting even a single live scan sample fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography as described in Section 6.2.4.1.

4.4.2 Biometric Data Representation and Protection

Biometric data shall be formatted using the standardized records specified in [SP 800-76]. The integrity of the mandatory fingerprint and optional iris and facial data records shall be protected using digital signatures as follows. The records shall be prepended with a Common Biometric Exchange Formats Framework (CBEFF) header (referred to as CBEFF_HEADER) and appended with the CBEFF signature block (referred to as the CBEFF_SIGNATURE_BLOCK) [CBEFF].

The format for CBEFF_HEADER is specified in [SP 800-76].

Deleted: to fingers

Deleted: SP800

Deleted: card fingerprints

Deleted: The format of the biometric record depends upon the biometric type (e.g., fingerprint, face, hand geometry). One or more records can be concatenated and prepended with a general record header to form a standard biometric record (referred to as STD_BIOMETRIC_RECORD). The standard biometric record is

Deleted:).

Deleted:]

The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus facilitates the verification of integrity of the biometric data. The process of generating a CBEFF_SIGNATURE_BLOCK is described as follows. The CBEFF_SIGNATURE_BLOCK shall be encoded as a CMS external digital signature as defined in [RFC5652]. The digital signature shall be computed over the entire CBEFF structure except the CBEFF_SIGNATURE_BLOCK itself (which means that it includes the CBEFF_HEADER and the biometric records). The algorithm and key size requirements for the digital signature are detailed in [SP 800-78].

The CMS encoding of the CBEFF_SIGNATURE_BLOCK is as a *SignedData* type, and shall include the following information:

- The message shall include a *version* field specifying version v3
- The *digestAlgorithms* field shall be as specified in [SP 800-78]
- The *encapcontentInfo* shall
  - Specify an *eContentType* of id-PIV-biometricObject
  - Omit the *eContent* field
- If the signature on the biometric was generated with the same key as the signature on the CHUID, the *certificates* field shall be omitted
- If the signature on the biometric was generated with a different key than the signature on the CHUID, the *certificates* field shall include only a single certificate, which can be used to verify the signature in the *SignerInfo* field
- The *crls* field shall be omitted
- *signerInfo*s shall be present and include only a single *SignerInfo*
- The *SignerInfo* shall
  - Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
  - Specify a *digestAlgorithm* in accordance with [SP 800-78]
  - Include at a minimum the following signed attributes:
    - A *MessageDigest* attribute containing the hash of the concatenated CBEFF_HEADER + Biometric Record
    - A *pivFASC-N* attribute containing the FASC-N of the PIV Card (to link the biometric data and PIV Card)
    - A *pivSigner-DN* attribute containing the subject name that appears in the PKI certificate for the entity that signed the biometric data
  - Include the digital signature.

The X.509 certificate containing the public key required to verify the digital signature shall be issued under the id-fpki-common-devices, id-fpki-common-hardware, or id-fpki-common-High policy of

Deleted: The complete CBEFF structure that contains the representation of the biometric data on the PIV Card consists of the following:¶ <#>CBEFF_HEADER¶ <#>STD_BIOMETRIC_RECORD¶ <#>CBEFF_SIGNATURE_BLOCK.¶ The format for CBEFF_HEADER and the STD_BIOMETRIC_RECORD is specified in [SP800-76].

Deleted: RFC3852

Deleted: STD_BIOMETRIC_RECORD).

Deleted: the same as those

Deleted: SP800

Deleted: as

Deleted: SP800

Deleted: STD_BIOMETRIC_

[COMMON].[15] The certificate shall also include an extended key usage (*extKeyUsage*) extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix D.

4.4.3 Biometric Data Content

Matching accuracy and data interoperability are the driving factors in specifying the biometric data on the PIV Card. These data characteristics include the image parameters (e.g., pixel density, pixel depth) in the image records as well as the fields in the encapsulating standard biometric record. As already stated, the biometric data content collected over the PIV life cycle shall conform to the specifications outlined in [SP 800-76].

4.5 Card Reader Requirements

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].

4.5.1 Contact Reader Requirements

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 physical access control 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.

4.5.2 Contactless Reader Requirements

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 contact card readers shall conform to the requirements specified in [SP 800-96]. In physical access control 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. This is necessary to allow retrofitting of PIV readers into existing physical access control systems that use a variety of non-standard card reader communication interfaces.

4.5.3 Reader Resilience and Flexibility

The international standard ISO/IEC 24727 [ISOIEC 24727] enables a high degree of interoperability between electronic credentials and relying subsystems by means of a firmware-defined 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.

[15] For legacy PKIs, as defined in Section 5.4.4, the certificates may be issued under a department or agency-specific policy that has been cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level.

Deleted:], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3.

Deleted: *extendedKeyUsage*

Deleted: This standard also requires that PIV biometric data is not readable in the clear and is protected through an authentication mechanism such as a PIN. However, this standard does not specify whether other biometric information should be stored in a contact or contactless IC. An electromagnetically opaque sleeve or other technology is required to protect against any unauthorized contactless access to biometric information stored on a contactless IC.¶

Deleted: SP800

Deleted: Specifications

Deleted: Specifications

Deleted: Specifications

Deleted: the [ISO 14443

Deleted: .

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

Deleted: Specifications

4.5.4 PIN Input Device Requirements

PIN input devices shall be used for implementing PIN-based PIV Card activation. When the PIV Card is used with a PIN for physical access, the PIN input device shall be integrated with the reader. When the PIV Card is used with a PIN for logical access (e.g., to authenticate to a Web site or other server), the PIN input device may be integrated with the reader or entered using the computer's keyboard. If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation.

5. PIV Key Management Requirements

PIV Cards consistent with this specification will have two or more asymmetric private keys. To manage the public keys associated with the asymmetric private keys, departments and agencies shall issue and manage X.509 public key certificates as specified below.

5.1 Architecture

The CA that issues certificates to support PIV Card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-signed, self-issued, and CA certificates issued by these CAs shall conform to *Worksheet 1: Self-Signed Certificate Profile*, *Worksheet 2: Self-Issued CA Certificate Profile*, and *Worksheet 3: Cross Certificate Profile*, respectively, in *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program* [PROF]. The requirements for legacy PKIs are defined in Section 5.4.

5.2 PKI Certificate

All certificates issued to support PIV Card authentication shall be issued under the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON]. The requirements in this certificate policy cover identity proofing and the management of CAs and registration authorities. CAs and registration authorities may be operated by departments and agencies, or may be outsourced to PKI service providers. For a list of PKI service providers that have been approved to operate under [COMMON], see http://www.idmanagement.gov/fpkipa/cpl.cfm.

[COMMON] requires FIPS 140 Level 2 validation for the subscriber cryptographic module (i.e., the PIV Card). In addition, this standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.

5.2.1 X.509 Certificate Contents

The required contents of X.509 certificates associated with PIV private keys are based on [PROF]. The relationship is described below:

- Certificates containing the public key associated with an asymmetric Card Authentication Key shall conform to *Worksheet 8: Card Authentication Certificate Profile* in [PROF].
- Certificates containing the public key associated with a digital signature private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF] and shall specify either the id-fpki-common-hardware or id-fpki-common-High policy in the certificate policies extension.
- Certificates containing the public key associated with a PIV authentication private key shall conform to *Worksheet 9: PIV Authentication Certificate Profile* in [PROF].

Deleted: Section Break (Next Page)

<#>PIV Card Issuance and Management Subsystem¶

This section defines the security requirements for processes that are part of the Card Issuance and Management Subsystem for a PIV-II implementation. These largely parallel the requirements for PIV-I, but includes the requirement for issuance and management of an interoperable PIV Card. 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 a PIV-II system are described in detail in Section 4 of this standard, NIST SP 800-73, and NIST SP 800-76.¶

<#>Control Objectives and Interoperability Requirements¶

[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 ... [1]

Deleted: one

Deleted: are required to

Deleted: *Common Policy*

Deleted: .4

Deleted: the id-CommonHW policy and the id-CommonAuth policy

Deleted: [16] as defined in

Deleted: for legacy PKIs are defined

Deleted: Section 5.4.4. These requirements

Deleted: who

Deleted: -2

Deleted: cryptomodule

Deleted: [COMMON] specifies the use of RSA along with the key sizes and hash functions. ¶ ... [2]

Deleted: <#>Authority Information Access (AIA) extensions shall include pointers to the appropriate OCSP s ... [3]

Deleted: must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extensior ... [4]

Deleted:].

Deleted: *5: End Entity Signature Certificate Profile* in [PROF], but shall not assert the nonRepudiation bit i ... [5]

- Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].[17]
- Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP 800-78].

Deleted: SP800
Deleted: [18]

5.3 X.509 CRL Contents

CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to *Worksheet 4: CRL Profile* in [PROF].

5.4 Migration from Legacy PKIs

For the purposes of this standard, legacy PKIs are the PKIs of departments and agencies that have cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level. PIV Authentication Certificates and Card Authentication Certificates issued by legacy PKIs shall meet the requirements specified in Section 5.2.1. Departments and agencies may assert department or agency-specific policy OIDs in PIV Authentication Certificates and Card Authentication Certificates in addition to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively. This specification imposes no requirements on digital signature or key management certificates issued by legacy PKIs.

Deleted: whose PKIs
Deleted: -HW,
Deleted: may continue to assert department or agency-specific policy Object Identifiers (OID).
Deleted: on or after January 1, 2008
Deleted: assert the id-CommonHW or id-CommonAuth policy OIDs. (
Deleted: continue to
Deleted: CommonHW and id-CommonAuth policy OIDs in
Deleted: after January 1, 2008.)

5.5 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 will be responsible for notifying Certification Authorities (CA) when cards or certificates need to be revoked. CAs shall maintain the status of servers and responders needed for PIV Card and certificate status checking.

Deleted: Certificate

The expiration date of the authentication certificates (PIV authentication certificate and Card authentication certificate) shall not be after the expiration date of the PIV Card. If the card is revoked, the authentication certificates shall 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 authentication certificate on a card is proof that the card was issued and is not revoked.

Deleted: certificate
Deleted: PIV

Because an authentication certificate typically is valid several years, a mechanism to distribute certificate status information is necessary. CRL and OCSP are the two commonly used mechanisms. CAs that issue authentication certificates shall maintain an LDAP directory server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it.

Deleted: certificates
Deleted: lasts
Deleted: certificate revocation
Deleted: Two
Deleted: conventional:
Deleted: CRL and the OCSP.

PIV Authentication key certificates and Card Authentication key certificates shall contain the *crlDistributionPoints* and *authorityInfoAccess* extensions needed to locate CRLs and the authoritative OCSP responder, respectively. In addition, every CA that issues these authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues.

Deleted: PIV
Deleted: a
Deleted: needed to build a path to the Federal Bridge CA
Deleted: or
Deleted: .
Deleted: PIV

[17] Note that Key Management certificates may assert the id-fpki-common-policy, id-fpki-common-hardware, or id-fpki-common-High policy in the certificate policies extension. Applications / relying systems sensitive to the assurance level may choose not to accept certificates that only assert id-fpki-common-policy.

5.5.1 Certificate and CRL Distribution

This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP). Specific requirements are found in the Shared Service Provider Repository Service Requirements [SSP REP].

Certificates that contain the FASC-N in the subject alternative name extension, such as PIV Authentication certificates and Card Authentication certificates, shall not be distributed publicly (e.g., via LDAP or HTTP accessible from the public Internet). Individual departments and agencies can decide whether other user certificates (digital signature and key management) can be distributed via LDAP. When user certificates are distributed, the requirements in Table IV—End-Entity Certificate Repository Service Requirements of [SSP REP] shall be satisfied.

Deleted: Table II—Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements of

Deleted: PIV Authentication certificates

Deleted: ; hence, these

Deleted: .

Deleted: I

5.5.2 OCSP Status Responders

OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status mechanism. The OCSP status responders must be updated at least as frequently as CRLs are issued. The definitive OCSP responder for each certificate shall be specified in the AIA extension as described in [PROF].

6. PIV Cardholder Authentication

This section defines a suite of identity authentication mechanisms that are supported by all the PIV Cards, and their applicability in meeting the requirements for a set of graduated levels of identity assurance. Specific implementation details of authentication mechanisms identified in this section are provided in [SP 800-73]. Moreover, while a wide range of authentication mechanisms is identified in this section, departments and agencies may adopt additional mechanisms that use the identity credentials on the PIV Card. In the context of the PIV Card Application, 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 granted to that identity for access to various physical and logical resources.

Deleted: Privacy Requirements¶
The PIV Privacy Requirements stated in Section 2.4 apply equally to PIV-II implementations.¶
Section Break (Next Page)

Deleted: PIV Card Holder

Deleted: Card

Deleted: that are

Deleted: to

6.1 Identity Authentication Assurance Levels

This standard defines three 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:

Deleted: .

Deleted: refers to the

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.
3) The strength of the technical mechanisms used to verify that the cardholder is the owner of the PIV Card.

Section 2 of this standard 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 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 identity authentication assurance levels defined in this standard:

Deleted: and 5

Deleted: define

Deleted: all

Deleted: . Hence, there is

Deleted: bears

Deleted: upon

Deleted: credentials

- 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) shall determine the appropriate level of identity assurance required for access, based on the harm and impact to individuals 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.

6.1.1 Relationship to OMB's E-Authentication Guidance

The levels of identity authentication assurance defined within this standard are closely aligned with Section 2 of OMB's E-Authentication Guidance for Federal Agencies, M-04-04 [OMB404]. Specifically,

Deleted: the discussion in

Table 6-1 shows the notional relationship between the PIV identity authentication assurance levels and the [OMB404] identity authentication assurance levels.

Table 6-1. Relationship Between PIV and E-Authentication Assurance Levels

OMB E-Authentication Levels		Comparable PIV Assurance Levels
Level Number	Description	
Level 2	Some confidence in the asserted identity's validity	SOME confidence
Level 3	High confidence in the asserted identity's validity	HIGH confidence
Level 4	Very high confidence in the asserted identity's validity	VERY HIGH confidence

[OMB404] addresses "four levels of identity assurance for electronic transactions requiring authentication" and prescribes a methodology for determining the level of identity assurance required based on the risks and potential impacts of errors in identity authentication. In the context of the PIV Card, owners of logical resources shall apply the methodology defined in [OMB404] to identify the level of identity authentication assurance required for their electronic transaction. Parties that are responsible for access to physical resources may use a methodology similar to that defined in [OMB404] to determine the PIV identity authentication assurance level required for access to their physical resource; they may also use other applicable methodologies to determine the required level of identity assurance for their application.

6.2 PIV Card Authentication Mechanisms

The following subsections define the basic types of authentication mechanisms that are supported by the credential set hosted by the PIV Card Application. PIV Cards can be used for identity authentication in environments that are equipped with card readers as well as those that lack card readers. Card readers, when present, can be contact readers or contactless readers. The usage environment affects the PIV identity authentication mechanisms that may be applied to a particular situation.

Each authentication mechanism described in this section is strengthened through the use of a back-end certificate status verification infrastructure. The status of the authentication certificates (i.e., PIV authentication certificate and Card authentication Certificate) is directly tied to the status of all other credential elements held by the card. Sections 6.2.1 through 6.2.4 define the basic types of authentication mechanisms that are supported by the core (mandatory) credential set on the PIV Card and are interoperable across agencies. Section 6.2.5 and section 6.2.6 define the authentication mechanisms that are available if the optional logical credential elements are present on the PIV Card.

Deleted: core (mandatory)

Deleted: . This standard does not define the authentication mechanisms that can be implemented using optional logical credential elements (e.g., symmetric authentication key) on the PIV Card. ¶

Deleted: The parameters of

Deleted: affect

Deleted: can be further

Deleted: if the access control point has connectivity to the department or agency's network infrastructure

6.2.1 Authentication Using PIV Visual Credentials (VIS)

Visual authentication of a PIV cardholder shall be used only to support access control to physical facilities and resources.

The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication, as follows:

- Zone 1F – Photograph

- Zone 2F – Name
- Zone 8F – Employee affiliation
- Zone 10F – Agency, Department or Organization
- Zone 14F – Expiration date
- Zone 1B – Agency card serial number (back of card)
- Zone 2B – Issuer identification number (back of card).

The PIV Card may also bear the following optional components:

- Zone 11F – Agency seal
- Zone 5B – Physical characteristics of cardholder
- Zone 3F –Signature.

When a cardholder attempts to pass through an access control point for a Federally controlled facility, a human guard shall perform visual identity verification of the cardholder, and determine whether the identified individual should be allowed through the control point. The series of steps that shall be applied in the visual authentication process are as follows:

1. The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way.
2. The guard compares the cardholder's facial features with the picture on the card to ensure that they match.
3. The guard checks the expiration date on the card to ensure that the card has not expired.
4. The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional)
5. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)
6. One or more of the other data elements on the card (e.g., name, employee affiliation, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Some characteristics of the visual authentication mechanism are as follows:

- Human inspection of card, which is not amenable for rapid or high volume access control
- Resistant to use of unaltered card by non-owner of card
- Low resistance to tampering and forgery

Deleted: employment identifier

Deleted: <#>Agency name and/or department¶
Department or

Deleted: PIV cardholder's

Deleted: Applicant's

Deleted: employment identifier

Deleted: of the

+ Applicable in environments with and without card readers.

6.2.2 Authentication Using the PIV CHUID

The PIV Card provides a mandatory logical credential called the CHUID. As described in Section 4.2, the CHUID contains numerous data elements.

The CHUID shall be used for PIV cardholder authentication using the following sequence:

1. The CHUID is read electronically from the PIV Card.
2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered.
3. The expiration date on the CHUID is checked to ensure that the card has not expired.
4. A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access.

Some characteristics of the CHUID-based authentication mechanism are as follows:

+ Can be used for rapid authentication for high volume access control
+ Low resistance to use of unaltered card by non-owner of card
+ Applicable with contact-based and contactless readers.

6.2.3 Authentication Using PIV Biometric

The PIV Card Application hosts the signed fingerprint templates and/or the signed iris image templates. Either biometric can be read from the card following cardholder-to-card (CTC) authentication using a PIN supplied by the cardholder. These PIV biometrics are designed to support a cardholder-to-external system (CTE) authentication mechanism through a match-off-card scheme. The following subsections define two authentication schemes that make use of the PIV biometrics. As noted in Section 4.4, neither the fingerprint template nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images are only required to be collected from cardholders whom fingerprints could not be collected. In some rare cases, a PIV Card may have neither fingerprint templates nor iris images, if neither fingerprints nor iris images could be collected from the cardholder.

Some characteristics of the PIV Biometrics authentication mechanisms (described below) are as follows:

+ Slower mechanism, because it requires two interactions (e.g., presentation of PIN and biometric) with the cardholder
+ Strong resistance to use of unaltered card by non-owner since PIN and cardholder biometric are required
+ Digital signature on biometric, which is checked to further strengthen the mechanism
+ Applicable only with contact-based card readers.

Deleted: (Optional)

Deleted: One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Numbering System [DUNS]) are

Deleted: of the

Deleted: a mandatory

Deleted: that

Deleted: The

Deleted: biometric is

Deleted: biometric

Deleted: of the

Deleted: Biometric

Deleted: is

Deleted: to activate card

Deleted: can be

6.2.3.1 Unattended Authentication Using PIV Biometric (BIO)

The following sequence shall be followed for unattended authentication of the PIV biometric:

1. The CHUID is read from the card.
2. The expiration date in the CHUID is checked to ensure the card has not expired.
3. The cardholder is prompted to submit a PIN, activating the PIV Card.
4. The PIV biometric is read from the card.
5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source.
6. The cardholder is prompted to submit a live biometric sample.
7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.
8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.
9. FASC-N is used as input to the authorization check to determine whether the cardholder should be granted access.

Deleted: (Optional)

Deleted: One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are

6.2.3.2 Attended Authentication of PIV Biometric (BIO-A)

The following sequence shall be followed for attended authentication of the PIV biometrics:

Deleted: biometric

1. The CHUID is read from the card.
2. The expiration date in the CHUID is checked to ensure that the card has not expired.
3. The cardholder is prompted to submit a PIN. The PIN entry is done in the view of an attendant.
4. The submitted PIN is used to activate the card. The PIV biometric is read from the card.
5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source.
6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in the view of an attendant.
7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.
8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric.
9. FASC-N is used as input to the authorization check to determine whether the cardholder should be granted access.

Deleted: (Optional)

Deleted: One or more of the CHUID data elements (e.g.,

Deleted: , Agency Code, DUNS) are

This authentication mechanism is similar to the unattended biometrics authentication mechanism; the only difference is that an attendant (e.g., security guard) supervises the use of the PIV Card and the submission of the PIN and the biometric by the cardholder.

Deleted: biometric credential check

Deleted: .

6.2.4 Authentication Using PIV Asymmetric Cryptography

Deleted: (PKI)

The PIV Card contains two mandatory asymmetric authentication private keys and corresponding certificates, as described in Section 4. The following subsections shall be used to perform authentication using the authentication keys. The PKI-Auth shall be the alternative authentication mechanism, in cases where neither the fingerprints nor its alternative iris images could be collect for on-card storage.

Deleted: carries a

Deleted: key

Deleted: certificate

Deleted: steps

Deleted: PIV asymmetric

Deleted: key:

6.2.4.1 Authentication with the PIV authentication certificate credential (PKI-AUTH)

1. The reader reads the PIV Authentication Key certificate from the PIV Card Application.
2. The cardholder is prompted to submit a PIN.
3. The submitted PIN is used to activate the card.
4. The reader issues a challenge string to the card and requests an asymmetric operation in response.
5. The card responds to the previously issued challenge by signing it using the PIV authentication private key.

Deleted: and attaching the associated certificate

6. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.
7. The response is validated as the expected response to the issued challenge.
8. The Subject Distinguished Name (DN) and unique identifier from the authentication certificate are extracted and passed as input to the access control decision.

Some of the characteristics of the PKI-based authentication mechanism are as follows:

+ Requires the use of online certificate status checking infrastructure
+ Highly resistant to credential forgery
+ Strong resistance to use of unaltered card by non-owner since PIN is required to activate card
+ Applicable with contact-based card readers.

6.2.4.2 Authentication with the Card authentication certificate credential (PKI-CAK)

1. The reader reads the Card Authentication Key (CAK) certificate from the PIV Card Application.
2. The reader issues a challenge string to the card and requests an asymmetric operation in response.

3. The card responds to the previously issued challenge by signing it using the card authentication private key.

4. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity.

5. The response is validated as the expected response to the issued challenge.

6. The FASC-N from the card authentication certificate is extracted and passed as input to the access control decision.

Some of the characteristics of the PKI-CAK authentication mechanism are as follows:

+ Requires the use of online certificate status checking infrastructure
+ Highly resistant to credential forgery
+ Applicable with contact-based and contactless readers.

Deleted: Subject Distinguished Name (DN) and

Deleted: are

Deleted: authorization function

Deleted: based

Deleted: ¶
Strong resistance to use of unaltered card by non-owner since PIN is required to activate card

Deleted: card

6.2.5 Authentication Using On-Card Biometric Comparison

The PIV Card Application may host the optional on-card biometric comparison algorithm. In this case, fingerprint templates are 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 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 mechanism to block this authentication mechanism after a number of consecutive failed authentication attempts as stipulated by department or agency. As with authentication using PIV biometric, aIf agencies choose to implement On-card biometric comparison it shall be implemented as defined in [SP 800-73] and [SP 800-76].

6.2.6 Authentication with the Symmetric Card Authentication Key

The PIV Card Application may host the optional symmetric card authentication key. In this case, the symmetric card authentication key shall be used for PIV cardholder authentication using the following sequence:

1. The CHUID is read electronically from the PIV Card.
2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered.
3. The expiration date on the CHUID is checked to ensure that the card has not expired.
4. The reader issues a challenge string to the card and requests a response.
5. The card responds to the previously issued challenge by signing it using the symmetric card authentication key.
6. The response is validated as the expected response to the issued challenge.

7. A unique identifier within the CHUID is used as input to the authorization check to determine whether the cardholder should be granted access.

6.3 PIV Support of Graduated Assurance Levels for Identity Authentication

The PIV Card supports a set of authentication mechanisms that can be used to implement graduated assurance levels for identity authentication. The following subsections specify the basic PIV authentication mechanisms that may be used to support the various levels of identity authentication assurance as defined in Section 6.1. Two or more complementing identity authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity.

Deleted: of the basic

Adequately designed and implemented relying systems can achieve the PIV Card authentication assurance levels stated in Tables 6-2 and 6-3. Less adequately designed or implemented relying systems may only achieve lower authentication assurance levels. The design of components of relying systems, including card readers, biometric readers, cryptographic modules, and key management systems, involves many factors not fully specified by FIPS 201, such as correctness of the functional mechanism, physical protection of the mechanism, and environmental conditions at the authentication point. Additional standards and best practice guidelines apply to the design and implementation of relying systems, e.g., FIPS 140 and SP 800-116.

6.3.1 Physical Access

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 6-2. An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

Deleted: can

Deleted: It is implicit that

Deleted: ¶
Each authentication mechanism described in the table can be further strengthened through the use of a back-end certificate status verification infrastructure, if the access control point has connectivity to the department or agency's network infrastructure.

Table 6-2. Authentication for Physical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism
SOME confidence	VIS, CHUID, PKI-CAK
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI-AUTH

Formatted Table

6.3.2 Logical Access

The PIV Card may be used to authenticate the cardholder in support of decisions concerning access to logical information resources. For example, a cardholder may log in to his or her department or agency network using the PIV Card; the identity established through this authentication process can be used for determining access to file systems, databases, and other services available on the network.

Table 6-3 describes the authentication mechanisms defined for this standard to support logical access control. An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

Deleted: It is implicit that

Table 6-3. Authentication for Logical Access

PIV Assurance Level Required by Application/Resource	Applicable PIV Authentication Mechanism	
	Local Workstation Environment	Remote/Network System Environment
SOME confidence	CHUID, PKI-CAK	PKI-CAK
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, PKI-AUTH	PKI-AUTH

Formatted Table

Deleted: ¶

Section Break (Next Page)

<#>PIV Processes¶

Sections 2.2 and 5.2 of this standard require the adoption and use an approved identity proofing and registration process. All identity proofing and registration systems must satisfy the PIV objectives and requirements stated in Sections 2.2 and 5.2 in order to be approved. ¶

¶

Section 2.3 and 5.3 of this standard requires the adoption and use of an approved credential issuance and management process. All credential issuance and management systems must satisfy the PIV objectives and requirements stated in Sections 2.3 and 5.3 in order to be approved. The heads of Federal departments and agencies may approve other identity proofing, registration and issuance process sets that are accredited as satisfying the requisite PIV objectives and requirements.¶

¶

Two examples of PIV identity proofing, registration and issuance process sets that satisfy the requisite PIV control objectives and requirements are provided in this Appendix. Wherever appropriate, additional PIV-II requirements have been specified in order to meet the objectives of PIV-II. ¶

¶

<#>Role Based Model¶

The role based identity proofing, registration and issuance process set is recommended for organizations not having a pre-existing PIV system.¶

¶

<#>PIV Identity Proofing and Registration¶

Departments and agencies that employ the generic process set for issuing PIV credentials shall follow the identity proofing and registration process defined in this section.¶

<#> Roles and Responsibilities¶

The critical roles associated with the PIV identity proofing, registration and issuance process are defined below. These roles may be ancillary roles assigned to personnel who have other primary duties. The following roles shall be employed for identity proofing and issuance: ¶

<#>**Applicant**—The individual to whom a PIV credential needs to be issued.¶

<#>**PIV Sponsor**—The individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.¶

<#>**PIV Registrar**—The entity responsible for identity proofing of the Applicant and ensuring the succes… [6]

Appendix A—PIV Validation, Certification, and Accreditation

A.1 Accreditation of PIV Card Issuers (PCI)

[HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process. To that end, NIST developed a set of attributes as the basis of reliability assessment of PIV Card Issuers (PCIs) in SP 800-79 and published this document in July 2005. Subsequent lessons learned in implementation experience (in credential management and PIV Card issuance) of various agencies together with the evolution of PCI organizations motivated NIST to develop a new accreditation methodology that is objective, efficient, and will result in consistent and repeatable accreditation decisions and published the substantial revision as SP 800-79-1 in June 2008 [SP 800-79]. The new PCI accreditation methodology is built on a foundation of four major Accreditation Topics, 13 Accreditation Focus Areas and a total of 79 Control requirements distributed under the various Accreditation Focus Areas. Associated with each control requirement are a set of assessment methods, the exercise of the latter will result in outcomes that form the basis for accreditation decisions.

The four major Accreditation Topics identified in [SP 800-79] are:

- Organizational Preparedness
- Security Management and Data Protection
- Infrastructure Elements
- (PIV) Processes

The entire spectrum of activities in the PCI accreditation methodology is divided into the following four phases:

- Initiation Phase
- Assessment Phase
- Accreditation Phase
- Monitoring Phase

The initiation phase involves communicating the goals of the assessment/accreditation to the key personnel of the PCI organization and the review of documents such as the PCI operations plan. In the assessment phase, the appropriate assessment methods stipulated in the methodology for each PCI control are carried out and the individual results recorded. The accreditation phase involves aggregating the results of assessment, arriving at an accreditation decision, and issuing the appropriate notification – Authorization to Operate (ATO) or the Denial of Authorization to Operate (DATO), that is consistent with the accreditation decision.

A.2 Security Certification and Accreditation of IT System(s) Supporting PCI

The accreditation of the capability and reliability of a PCI using the methodology outlined in [SP 800-79] depends upon adequate security for the information systems that are used for PCI functions. The assurance that such a security exists in a PCI is obtained through security certification and accreditation of IT systems performed using the methodology specified in SP 800-37. [SP 800-37] The methodology in

Deleted: Service Providers

Deleted: Funding permitting

Deleted: will establish detailed criteria that

Deleted: issues must meet

Deleted: . Additionally, NIST will (again, funding permitting) establish a government-wide program to accredit official issuers of PIV Cards against these accreditation criteria. Until

Deleted: time as these are completed, agencies must self-certify their own issuers of PIV Cards.

Deleted: In order to accomplish the accreditation of PIV service providers as described above, and to be compliant with the provisions of OMB Circular A-130, App. III, the IT system(s) used by PIV service providers must also be certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems. Security certification is a comprehensive assessment of the management, operational, and technical security controls in an information system. NIST SP 800-37 provides a formal framework for certification, along with specific requirements for validating and obtaining certificates for the PIV modules described below. [SP800-37] ¶

[SP 800-37] in turn was created in pursuant to a mandate in Appendix III of Office of Management and Budget (OMB) Circular A-130. An accreditation decision granted under [SP 800-37] signifies that a PCI organization's official accepts responsibility for the security (in terms of confidentiality, integrity, and availability of information) of the information systems that will be involved in carrying out the PCI functions. Hence accreditation under [SP 800-37] is mandatory for issuing PCI accreditation using SP 800-79.

A.3 Conformance of PIV Card Application and Middleware Testing to Specifications Based on this Standard

Assurance of conformance of the PIV Card Application and PIV Middleware interfaces to this standard and its associated technical specifications is needed in order to meet the security and interoperability goals of HSPD-12. To facilitate this, NIST has established the NIST Personal Identity Verification Program (NPIVP). Under this program NIST has developed test procedures in SP 800-85A, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)*, and an associated toolkit for conformance testing of PIV Card Application and PIV Middleware. [SP 800-85A] Commercial products under these two categories are tested by the set of accredited test laboratories, accredited under National Voluntary Laboratory Accreditation Program (NVLAP) program, using the NIST supplied test procedures and toolkit. The outcomes of the test results are validated by NIST, which then issues validation certificates. Information about NPIVP is available at http://csrc.nist.gov/groups/SNS/piv/npivp.

A.4 Cryptographic Testing and Validation (FIPS 140 and algorithm standards)

All on-card cryptographic modules hosting the PIV Card Application and cryptographic modules of Card Issuance and Maintenance Systems shall be validated to FIPS 140 with an overall Security Level 2 (or higher). [FIPS140-2] The facilities for FIPS 140 testing are the Cryptographic and Security Testing (CST) laboratories accredited by the NVLAP program of NIST. Vendors wanting to supply cryptographic modules 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), 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/index.html.

A.5 FIPS 201 Evaluation Program

In order to evaluate the conformance of different families of products that support the PIV processes to this standard and its associated technical specifications, the Office of Government-wide Policy (OGP) under GSA set up the FIPS 201 Evaluation Program. The product families include Card Personalization products, Card Readers, Products involved in Credential enrollment functions such as Fingerprint and Facial Image Capture equipments, Biometric fingerprint template generators etc. Products evaluated and approved under this program are placed on the FIPS 201 Approved Products List (APL) to enable procurement of conformant products by implementing agencies. The details of the program are available at http://fips201ep.cio.gov/.

Deleted: Components to

Deleted: NIST plans to develop a PIV validation program that will test implementations for conformance with this standard. Note that the following is not requirements until NIST establishes a program. Information on this program will be published at as it becomes available.¶
A PIV system is FIPS 201-compliant after each of its constituent components (card, reader, issuer software, and registration database) has met its individual validation requirements. Because these individual validation requirements are based on different standards and no single test laboratory is accredited for validating products built to all these standards, a PIV system has to undergo testing and consequent validation through multiple validation facilities. The PIV components and currently available validation requirements are summarized in Table B-1.¶
¶
Table B-1. PIV System Components and Validation Requirements¶
PIV Component ... [7]

Deleted: -2

Deleted: the

Deleted: in

Deleted: system (both on-card

Deleted: issuer software)

Deleted: -2

Deleted: -2

Deleted: National Voluntary Laboratory Accreditation Program ()

Deleted: for the PIV system

Deleted: ncsl.

Deleted: cryptval

Appendix B—Background Check Descriptions

The following describes the details of a National Agency Check with Inquiries (NACI).

Deleted: (NAC) and a National Agency Check

+ **NACI.** The basic and minimum investigation required on all new Federal employees consisting of a National Agency Check (NAC) with written inquiries and searches of records covering specific areas of an individual's background during the past five years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities). Coverage includes:

Deleted: <#>**NAC.** The NAC is part of every NACI. Standard NACs are Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check.¶

Deleted: NAC

  - Employment, 5 years
  - Education, 5 years and highest degree verified
  - Residence, 3 years
  - References
  - Law Enforcement, 5 years
  - NACs

Appendix C—PIV Card Processes

The following table is a summary of the requirements described in Section 2.4 and Section 2.5. The summary is provided as an overview of the requirements and is only intend to be a quick reference.

FIPS 201-2 Card Processes and Their Requirements								
	Issuance	Maintenance						
	Issuance	Renewal		Reissuance		Re-Key	Post Issuance Updates	
		Data Change	No Data Change	Data Change	No Data Change			
Sponsor Approval	●	●	●	● (if expiration date is extended)	● (if expiration date is extended)			
Identity Proofing	●							
Biometric Collection	●	Good for 12 years	Good for 12 years	Good for 12 years	Good for 12 years			
Enroll in Chain-of-trust	●	Record change		Record change				
NCHC	●							
NACI	●	●	●	● (if expiration date is extended)	● (if expiration date is extended)			
Chain-of-trust verification (CV)	●	●	●	●	●		● (if biometric data change)	
Valid PIV Card in Possession		●	●	● (unless lost/stolen)		●		●
New Physical Card issued (new FASC-N)	●	●	●	●	●			
Re-enrollment if CV not available		●	●	●	●			
Expiration Date	Maximum 6 yrs	Maximum 6 yrs	Maximum 6 yrs	Maximum 6 yrs	Maximum 6 yrs	No Change	No Change	

Appendix D—PIV Object Identifiers and Certificate Extension

D.1 PIV Object Identifiers

Table D-1 lists details for PIV object identifiers.

Table D-1. PIV Object Identifiers

ID	Object Identifier	Description
PIV eContent Types		
id-PIV-CHUIDSecurityObject	2.16.840.1.101.3.6.1	The associated content is the concatenated contents of the CHUID, excluding the authentication key map and the asymmetric signature field.
id-PIV-biometricObject	2.16.840.1.101.3.6.2	The associated content is the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD.
PIV Attributes		
pivCardholder-Name	2.16.840.1.101.3.6.3	The attribute value is of type DirectoryString and specifies the PIV cardholder's name.
pivCardholder-DN	2.16.840.1.101.3.6.4	The attribute value is an X.501 type Name and specifies the DN associated with the PIV cardholder in the PIV certificate(s).
pivSigner-DN	2.16.840.1.101.3.6.5	The attribute value is an X.501 type Name and specifies the subject name that appears in the PKI certificate for the entity that signed the biometric or CHUID.
pivFASC-N	2.16.840.1.101.3.6.6	The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures. Where used as a name type, the syntax is OCTET STRING. Where used as an attribute, the attribute value is of type OCTET STRING. In each case, the value specifies the FASC-N of the PIV Card.
PIV Extended Key Usage		
id-PIV-content-signing	2.16.840.1.101.3.6.7	This specifies that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics.
id-PIV-cardAuth	2.16.840.1.101.3.6.8	This specifies that the public key is used to authenticate the PIV Card rather than the PIV cardholder.

Deleted: +

D.2 PIV Certificate Extension

The PIV NACI indicator is a non-critical extension that may appear in PIV authentication certificates and card authentication certificates. The PIV NACI indicator extension indicates the status of the subject's background investigation at the time of credential issuance. The value of this extension is asserted as follows:

Deleted: The PIV NACI indicator extension is always non-critical, and SHALL appear in all PIV authentication certificates.

+ TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed successfully, and (2) a NACI has been initiated but has not completed.

+ FALSE if, at the time of credential issuance, the subject's NACI has been completed and successfully adjudicated.

The PIV NACI indicator extension is identified by the id-piv-NACI object identifier. The syntax for this extension is defined by the following ASN.1 module.

```
PIV-Cert-Extensions { 2 16 840 1 101 3 6 10 1  }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NONE --

id-piv-NACI OBJECT IDENTIFIER  ::= { 2 16 840 1 101 3 6 9 1 }

NACI-indicator ::= BOOLEAN

END
```

Deleted: Note that PIV authentication certificates MUST NOT be issued to a subject if —¶
<#>a NACI has been completed unsuccessfully;¶
<#>the FBI National Criminal History Fingerprint Check has not completed; or¶
<#>a NACI has not yet been initiated.¶

Deleted: See an important at the end of this document.

Deleted: _

Deleted: _

Deleted: _

Deleted: DEFAULT FALSE

Appendix E—Glossary of Terms, Acronyms, and Notations

E.1 Glossary of Terms

The following terms are used throughout this standard.

Access Control: The process of granting or denying specific requests: 1) obtain and use information and related information processing services; and 2) enter specific physical facilities (e.g., Federal buildings, military establishments, border crossing entrances).

Applicant: An individual applying for a PIV Card/credential. The Applicant may be a current or prospective Federal hire, a Federal employee, or a contractor.

Application: A hardware/software system implemented to satisfy a particular set of requirements. In this context, an application incorporates a system used to satisfy a subset of requirements related to the verification or identification of an end user's identity so that the end user's identifier can be used to facilitate the end user's interaction with the system.

Approved: FIPS approved or NIST recommended. An algorithm or technique that is either (1) specified in a FIPS or a NIST recommendation or (2) adopted in a FIPS or NIST recommendation.

Architecture: A highly structured specification of an acceptable approach within a framework for solving a specific problem. An architecture contains descriptions of all the components of a selected, acceptable solution while allowing certain details of specific components to be variable to satisfy related constraints (e.g., costs, local environment, user acceptability).

Assurance Level (or E-Authentication Assurance Level): A measure of trust or confidence in an authentication mechanism defined in OMB Memorandum M-04-04 and NIST Special Publication (SP) 800-63, in terms of four levels: [M-04-04]

- Level 1: LITTLE OR NO confidence
- Level 2: SOME confidence
- Level 3: HIGH confidence
- Level 4: VERY HIGH confidence

Asymmetric Keys: Two related keys, a public key and a private key, that are used to perform complementary operations, such as encryption and decryption or signature generation and signature verification.

Authentication: The process of establishing confidence of authenticity; in this case, in the validity of a person's identity and the PIV Card.

Biometric: A measurable, physical characteristic or personal behavioral trait used to recognize the identity, or verify the claimed identity, of an Applicant. Facial images, fingerprints, and iris scan samples are all examples of biometrics.

Biometric Information: The stored electronic information pertaining to a biometric. This information can be in terms of raw or compressed pixels or in terms of some characteristic (e.g., patterns).

Biometric System: An automated system capable of the following:

Deleted: <#>Physical Access Control Mechanisms¶

The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group publication *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* (PACS) provides guidance on physical access for various assurance profiles. Table C-1 describes the relationship between the PACS assurance levels and the PIV identity authentication levels defined in Section 6.1.¶

¶

Table E-1. PIV Support of PACS Assurance Profiles ¶

PACS Assurance Profile ... [8]

Deleted: iriscan

- Capturing a biometric sample from an end user
- Extracting biometric data from that sample
- Comparing the extracted biometric data with data contained in one or more references
- Deciding how well they match
- Indicating whether or not an identification or verification of identity has been achieved.

Capture: The method of taking a biometric sample from an end user. [INCITS/M1-040211]

Cardholder: An individual possessing an issued PIV Card.

Certificate Revocation List: A list of revoked public key certificates created and digitally signed by a Certification Authority. [RFC 5280]

Deleted: 3280

Certification: The process of verifying the correctness of a statement or claim and issuing a certificate as to its correctness.

Certification Authority: A trusted entity that issues and revokes public key certificates.

Chain-of-trust: The chain-of-trust is a sequence of related enrollment data sets that is created and maintained by PIV Card issuers.

Claimant: A party whose identity is to be verified using an authentication protocol.

Comparison: The process of comparing a biometric with a previously stored reference. See also "Identification" and "Identity Verification". [INCITS/M1-040211]

Component: An element of a large system, such as an identity card, PIV Issuer, PIV Registrar, card reader, or identity verification support, within the PIV system.

Conformance Testing: A process established by NIST within its responsibilities of developing, promulgating, and supporting FIPS for testing specific characteristics of components, products, and services, as well as people and organizations for compliance with a FIPS.

Credential: Evidence attesting to one's right to credit or authority; in this standard, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.

Cryptographic Key (Key): A parameter used in conjunction with a cryptographic algorithm that determines the specific operation of that algorithm.

Enrollment data set: A record including information about a biometric enrollment: name and role of the acquiring agent, office and organization, time, place, and acquisition method.

Federal Agency Smart Credential Number (FASC-N): As required by FIPS 201, the primary identifier on the PIV Card for physical access control. The FASC-N is a fixed length (25 byte) data object, specified in [SP 800-73], and included in several data objects on a PIV Card.

FASC-N Identifier: The FASC-N shall be in accordance with [SP 800-73]. A subset of FASC-N, a FASC-N Identifier, is a unique identifier as described in [SP 800-73].

Federal Information Processing Standards (FIPS): A standard for adoption and use by Federal departments and agencies that has been developed within the Information Technology Laboratory and published by NIST, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology to achieve a common level of quality or some level of interoperability.

Framework: A structured description of a topic of interest, including a detailed statement of the problem(s) to be solved and the goal(s) to be achieved. An annotated outline of all the issues that must be addressed while developing acceptable solutions to the problem(s). A description and analysis of the constraints that must be satisfied by an acceptable solution and detailed specifications of acceptable approaches to solving the problems(s).

Graduated Security: A security system that provides several levels (e.g., low, moderate, high) of protection based on threats, risks, available technology, support services, time, human concerns, and economics.

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Approved hash functions satisfy the following properties:

1. **One-Way.** It is computationally infeasible to find any input that maps to any pre-specified output.
2. **Collision Resistant.** It is computationally infeasible to find any two distinct inputs that map to the same output.

Deleted: Hash-Based Message Authentication Code (HMAC): A message authentication code that uses a cryptographic key in conjunction with a hash function.¶

Identification: The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Identifier: Unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.

Identity: The set of physical and behavioral characteristics by which an individual is uniquely recognizable.

Identity Authentication Assurance Level: A degree of confidence established in the identity of the holder of the PIV Card.

Identity Binding – Binding of the vetted claimed identity to the individual (through biometrics) according to the issuing authority. Represented by an identity assertion from the issuer that is carried by a *PIV credential*.

Identity Management System (IDMS) – Identity management system comprised of one or more systems or applications that manages the identity verification, validation, and issuance process.

Identity Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) to a PIV Registrar when attempting to establish an identity.

Identity Registration: The process of making a person's identity known to the PIV system, associating a unique identifier with that identity, and collecting and recording the person's relevant attributes into the system.

Identity Verification: The process of confirming or denying that a claimed identity is correct by comparing the credentials (something you know, something you have, something you are) of a person requesting access with those previously proven and stored in the PIV Card or system and associated with the identity being claimed.

Information in Identifiable Form (IIF): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. [E-Gov]

Interoperability: For the purposes of this standard, interoperability allows any government facility or information system, regardless of the PIV Issuer, to verify a cardholder's identity using the credentials on the PIV Card.

Issuer: The organization that is issuing the PIV Card to an Applicant. Typically this is an organization for which the Applicant is working.

Key: See "Cryptographic Key".

Deleted: **JPEG:** A standardized image compression function originally established by the Joint Photographic Experts Group.¶

Match/Matching: The process of comparing biometric information against a previously stored biometric data and scoring the level of similarity.

Model: A very detailed description or scaled representation of one component of a larger system that can be created, operated, and analyzed to predict actual operational characteristics of the final produced component.

Deleted: **Message Authentication Code (MAC):** A cryptographic checksum on data that uses a symmetric key to detect both accidental and intentional modifications of the data.¶

Off-Card: Refers to data that is not stored within the PIV Card or to a computation that is not performed by the Integrated Circuit Chip (ICC) of the PIV Card.

On-Card: Refers to data that is stored within the PIV Card or to a computation that is performed by the Integrated Circuit Chip (ICC) of the PIV Card.

One-to-Many: Synonym for "Identification". [INCITS/M1-040211]

Online Certificate Status Protocol (OCSP): An online protocol used to determine the status of a public key certificate. [RFC 2560]

Path Validation: The process of verifying the binding between the subject identifier and subject public key in a certificate, based on the public key of a trust anchor, through the validation of a chain of certificates that begins with a certificate issued by the trust anchor and ends with the target certificate. Successful path validation provides strong evidence that the information in the target certificate is trustworthy.

Personal Identification Number (PIN): A secret that a claimant memorizes and uses to authenticate his or her identity.

Deleted: PINs are generally only decimal digits.

Personal Identity Verification (PIV) Card: A physical artifact (e.g., identity card, "smart" card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the cardholder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).

PIV Issuer: An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.

PIV Registrar: An entity that establishes and vouches for the identity of an Applicant to a PIV Issuer. The PIV Registrar authenticates the Applicant's identity by checking identity source documents and identity proofing, and ensures a proper background check has been completed, before the credential is issued.

PIV Sponsor: An individual who can act on behalf of a department or agency to request a PIV Card for an Applicant.

Population: The set of users for the application. [INCITS/M1-040211]

Pseudonyms: a name assigned by a Federal Department or Agency through a formal process to a Federal employee for the purpose of the employee's protection (i.e., the employee might be placed at risk if their actual name were known) or for other purposes.

Public Key: The public part of an asymmetric key pair that is typically used to verify signatures or encrypt data.

Public Key Infrastructure (PKI): A support service to the PIV system that provides the cryptographic keys needed to perform digital signature-based identity verification and to protect communications and storage of sensitive verification system data within identity cards and the verification system.

PKI-Card Authentication Key (PKI-CAK): A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the Card authentication key of the PIV card and a contact or contactless reader.

PKI-PIV Authentication Key (PKI-AUTH): A PIV authentication mechanism that is implemented by an asymmetric key challenge/response protocol using the PIV authentication key of the PIV card and a contact reader.

Recommendation: A special publication of the ITL stipulating specific characteristics of technology to use or procedures to follow to achieve a common level of quality or level of interoperability.

Reference Implementation: An implementation of a FIPS or a recommendation available from NIST/ITL for demonstrating proof of concept, implementation methods, technology utilization, and operational feasibility.

Registration: See "Identity Registration".

Secret Key: A cryptographic key that must be protected from unauthorized disclosure to protect data encrypted with the key. The use of the term "secret" in this context does not imply a classification level; rather, the term implies the need to protect the key from disclosure or substitution.

Standard: A published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.

Trustworthiness – Security decision with respect to extended investigations to determine and confirm qualifications, and suitability to perform specific tasks and responsibilities.

Validation: The process of demonstrating that the system under consideration meets in all respects the specification of that system. [INCITS/M1-040211]

Verification: See "Identity Verification".

E.2 Acronyms

The following acronyms and abbreviations are used throughout this standard:

ACL	Access Control List
AES	Advanced Encryption Standard
AIA	Authority Information Access
AIM	Association for Automatic Identification and Mobility
ANSI	American National Standards Institute
CA	Certification Authority
CAK	**Card Authentication Key**
CBEFF	Common Biometric Exchange Formats Framework
CFR	Code of Federal Regulations
CHUID	Cardholder Unique Identifier
CMS	Cryptographic Message Syntax
CMT	Cryptographic Module Testing
CMTC	Card Management System to the Card
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
CRL	Certificate Revocation List
CSE	Communication Security Establishment
CTC	Cardholder to Card
CTE	Cardholder to External System
CVS	Clearance Verification System
DHS	Department of Homeland Security
DN	Distinguished Name
dpi	Dots Per Inch
ECC	Elliptic Curve Cryptography
ERT	Emergency Response Team
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FICC	Federal Identity Credentialing Committee
FIPS	Federal Information Processing Standards
FIPS PUB	FIPS Publication
FISMA	Federal Information Security Management Act
HSPD	Homeland Security Presidential Directive

Deleted: CIA . Cryptographic Information Application¶

Deleted: ¶
DCII . Defense

Deleted: and Investigation Index

Deleted: DUNS . Data Universal Numbering System¶

Deleted: ECDH . Elliptic Curve Diffie-Hellman¶
ECDSA . Elliptic Curve Digital Signature Algorithm¶

Deleted: Certificate

Deleted: HMAC . Hash-Based Message Authentication Code¶
HR . House of Representatives¶

HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IAB	Interagency Advisory Board
ICC	Integrated Circuit Chip
ID	Identification
IDMS	Identity Management System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIF	Information in Identifiable Form
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NCHC	National Criminal History Check
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NPIVP	NIST Personal Identity Verification Program
NVLAP	National Voluntary Laboratory Accreditation Program
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCI	PIV Card Issuer
PC/SC	Personal Computer/Smart Card
PDF	Portable Data File
PIA	Privacy Impact Assessment
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
RSA	Rivest Shamir Adleman
SAVE	Systematic Alien Verification for Entitlements
SF	Standard Form
SP	Special Publication
TSA	Transportation Security Administration
USCIS	U.S. Citizenship and Immigration Services

Deleted: **JPEG** . Joint Photographic Experts Group¶
¶

Deleted: **MAC** . Message Authentication Code¶
MQV . Menezes-Qu-Vanstone¶
¶

Deleted: **PACS** . Physical Access Control System¶

Deleted: **pt** . Point¶

Deleted: Comment

Deleted: **SHA** . Secure Hash Algorithm¶
SII . Security/Suitability Investigations Index¶

Deleted: **SSP REP** . Shared Service Provider Repository Service Requirement¶
¶
URI . Uniform Resource Identifier¶

E.3 Notations

This standard uses the following typographical conventions in text:

- ASN.1 data types are represented in *italics*. For example, *SignedData* and *SignerInfo* are data types defined for digital signatures.
- Letters or words in CAPITALS separated with underscore represent CBEFF-compliant data structures. For example, CBEFF_HEADER is a header field in the CBEFF structure.

Deleted: The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this standard are to be interpreted as described in IETF RFC 2119.¶ Additionally,

Deleted: Terms (word or concatenated words) in *Italics* represent

Deleted: .

Deleted: *or*

Appendix F—References

[ANSI322] ANSI INCITS 322 Information Technology, *Card Durability Test Methods*, ANSI, 2002.

[CBEFF] NISTIR 6529-A, *Common Biometric Exchange Formats Framework (CBEFF)*, NIST, 2003.

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 3647 – 1.12, October 15, 2010, or as amended. Available at http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf.

[E-Gov] *E-Government Act of 2002*, U.S. Public Law 107-347, 2002.

[EO10450] Executive Order 10450, *Security Requirements for Government Employees*, April 17, 1953. Available at http://www.dss.mil/nf/adr/10450/eo10450T.htm.

[FIPS140] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001, or as amended. Available at http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf.

[G155-00] ASTM G155-00, *Standard Practice for Operating Xenon Arc Light Apparatus for Exposure of Non-metallic Materials*, Vol. 14.04, ASTM, July 2000.

[G90-98] ASTM G90-98, *Standard Practice for Performing Accelerated Outdoor Weathering of Non-metallic Materials Using Concentrated Natural Sunlight*, Vol. 14.04, ASTM, 2003.

[HSPD-12] HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004.

[INCITS/M1-040211] ANSI/INCITS M1-040211, *Biometric Profile—Interoperability and Data Interchange—Biometrics-Based Verification and Identification of Transportation Workers*, ANSI, April 2004.

[ISO10373] ISO/IEC 10373, *Identification Cards—Test Methods*. Part 1—*Standard for General Characteristic Test of Identification Cards*, ISO, 1998. Part 3—*Standard for Integrated Circuit Cards with Contacts and Related Interface Devices*, ISO, 2001. Part 6—*Standard for Proximity Card Support in Identification Cards*, ISO, 2001.

[ISO14443] ISO/IEC 14443-1:2000, *Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards*, ISO, 2000.

[ISO7810] ISO/IEC 7810:2003, *Identification Cards—Physical Characteristics*, ISO, 2003.

[ISO7816] ISO/IEC 7816, *Identification Cards—Integrated Circuits with Contacts*, Parts 1-6, ISO.

[MRTD] International Civil Aviation Organization. *PKI for Machine Readable Travel Documents offering ICC Read-Only Access.* Version – 1.1, October 2004.

Deleted: 2.0, November
Deleted: , 2004.
Deleted: cio
Deleted: ficc
Field Code Changed
Deleted: -2

[NISTIR7123] NISTIR 7123, *Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report*, NIST, June 2004.

[OMB322] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003.

[OMB404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB, December 2003.

[PCSC] Personal Computer/Smart Card Workgroup Specifications. Available at http://www.pcscworkgroup.com.

[PRIVACY] *Privacy Act of 1974*, U.S. Public Law 93-579, 1974.

[PROF] *X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Provider (SSP) Program*, Version 1.5, January 7, 2008 or as amended. Available at http://www.idmanagement.gov/fpkipa/documents/CertCRLprofileForCP.pdf.

[RFC2560] RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP*, Internet Engineering Task Force (IETF), June 1999. Available at http://www.ietf.org/rfc/rfc2560.txt.

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

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

[SP 800-37] NIST Special Publication 800-37-1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, NIST, February 2010 or as amended.

[SP 800-53] NIST Special Publication 800-53-3, *Recommended Security Controls for Federal Information Systems and Organizations*, NIST, August 2009 or as amended.

[SP 800-63] NIST Special Publication 800-63 Version 1.0.2, *Electronic Authentication Guideline*, Appendix A, NIST, April 2006 or as amended.

[SP 800-73] NIST Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, NIST, February 2010 or as amended.

[SP 800-76] NIST Special Publication 800-76-1, *Biometric Data Specification for Personal Identity Verification*, NIST, January 2007 or as amended

[SP 800-78] NIST Special Publication 800-78-2, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, February 2010 or amended.

[SP 800-79] NIST Special Publication 800-79-1, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, NIST, June 2008 or amended.

[SP 800-85A] NIST Special Publication 800-85A-2, *PIV Card Application and Middleware Interface Test Guidelines (SP800-73-3 compliance)*, NIST, August 2010 or amended.

Deleted: [PACS] PACS v2.2, *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems*, Version 2.2, The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group, July 27, 2004.¶

Deleted: *Common Policy*

Deleted: 1, July 8, 2004.

Deleted: *(*

Deleted: *),*

Deleted: RFC3280

Deleted: 3280

Deleted: April 2002

Deleted: RFC3852

Deleted: 3852

Deleted: July 2004

Deleted: SP800

Deleted: *Security Certification and Accreditation of*

Deleted: , NIST, May 2004

Deleted: SP800

Deleted: September 2004 (2PD).

Deleted: SP800

Deleted: June 2004

Deleted: SP800

Deleted: , *Integrated Circuit Card*

Deleted: 2005

Deleted: SP800

Deleted: February 2006.

Deleted: SP800

Deleted: March 2005

[SP 800-87] NIST Special Publication 800-87 Revision 1, *Codes for the Identification of Federal and Federally-Assisted Organizations*, NIST, April 2008 or amended.

[SP 800-96] NIST Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*, NIST, September 2006 or amended.

[SP 800-116] NIST Special Publication 800-116, *A Recommendation for the use of PIV Credentials in Physical Access Control Systems (PACS)*, NIST, November 2008 or amended.

[SP 800-122] NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), NIST, April 2010 or amended.

[SPRINGER MEMO] Final Credentialing Standards for Issuing Personal Identity Verification Cards under HSPD-12, July 31, 2008.

[SSP REP] Shared Service Provider Repository Service Requirements, June 28, 2007, or as amended. Available at http://www.idmanagement.gov/fpkipa/documents/SSPrepositoryRqmts.pdf.

Deleted: January 23, 2004

Deleted: Section Break (Next Page)
FIPS 201-1, PERSONAL IDENTITY VERIFICATION (PIV) OF FEDERAL EMPLOYEES AND CONTRACTORS¶
CHANGE NOTICE 1¶
¶
U.S. DEPARTMENT OF COMMERCE¶
NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY¶
Gaithersburg, MD 20899¶
DATE OF CHANGE: June 23, 2006¶
Questions regarding this change notice may be directed to or to William MacGregor (, 301-975-8721). ¶
The Homeland Security Presidential Directive HSPD-12 called for a common identification standard to be adopted governing the interoperable use of identity credentials to allow physical and logical access to Federal government locations and systems. The Personal Identity Verification (PIV) of Federal Employees and Contractors, Federal Information Processing Standard 201 (FIPS 201-1) was developed to establish standards for identity credentials. This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems. ¶
FIPS 201-1 was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on March 2006. This change notice provides changes to the graphics on the back of the PIV card and the ASN.1 encoding of NACI indicator as follows:¶

Appendix G—Revision History

The Revision History is a complete list of updates to FIPS 201 since its initial release.

Version	Release Date	Updates
FIPS 201	February 2005	Initial Release
FIPS 201-1	March 2006	Added the requirement for electronically distinguishable from identity credentials issued to individuals who have a completed investigation (NACI Indictor).
FIPS 201-1 Change Notice 1	March 2006	Added clarification for variable placement of Agency Card Serial Number along the outer edge of the back of the PIV Card is allowed. Also, updated ASN.1 encoding for NACI Indicator.
FIPS 201-2, Draft	March 2011	This version represents 5 year review of FISP 201 and change request inputs received from agencies. Following is the highlights of changes made in this version. Incorporated reference to the memo by Linda Springer, Director OPM, dated 31 Jul 2008 for Credentialing Requirements. Incorporated the content from the I-9 form that is relevant to FIPS 201. Introduced the concept of a "chain-of-trust" maintained by a PIV Card Issuer. The "chain-of-trust" allows the owner of a PIV Card to obtain a replacement for a compromised, lost, stolen, or damaged PIV Card through biometric authentication. Changed the maximum life of PIV Card from 5 years to 6 years. Introduced a special rule for pseudonyms. Introduced a grace period for the period between termination of an employee or contractor and re-employment by the US Government or a USG Federal contractor. Revised the PIV Card Issuance and Maintenance requirements based on above changes. Added requirements for post-issuance updates. Incorporated visual card topography zones and color specifications from SP 800-104 and added clarifications to some of the existing zones. Added optional requirements for Section 508 compliance. Introduced requirement to collect alternate iris images when an agency cannot capture reliable fingerprints. Made asymmetric card authentication key mandatory and symmetric card authentication key optional. Added optional On-card biometric comparison as a means of performing card activation and PIV authentication mechanism. Inserted hook for additional keys if they are needed for

Deleted: Date
Formatted Table
Deleted: Section, Page
Deleted: Clarification
Deleted: 4.1.4.2, Pg. 18
Deleted: 6/23/06
Deleted: Variable placement
Deleted: Agency Card Serial Number along
Formatted Table
Deleted: outer edge
Deleted: back of
Deleted: is allowed.
Deleted: Figure 4-6 and Figure 4-8 below further clarifies the placement of Agency Card Serial Number

		secure messaging. Modified card activation to allow for PIN or equivalent verification data (e.g., biometric data). Added an option to include country(ies) of citizenship of Foreign Nationals in the PIV Authentication Certificate. Require signature verification and certificate path validation in the CHUID, BIO, and BIO-A authentication mechanisms. Added support for On-card Biometric Comparison Removed Annex A which provided two examples of PIV Processes.

Deleted: 6/23/06¶ ... [9]

Deleted: ¶

¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶

Figure 4-6. Card Back—Printable Areas and Required Data¶

Page Break

<sp>¶

¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶
¶

Figure 4-8. Card Back—Optional Data Placement—Example 2

Section Break (Next Page)

PIV Card Issuance and Management Subsystem

This section defines the security requirements for processes that are part of the Card Issuance and Management Subsystem for a PIV-II implementation. These largely parallel the requirements for PIV-I, but includes the requirement for issuance and management of an interoperable PIV Card. 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 a PIV-II system are described in detail in Section 4 of this standard, NIST SP 800-73, and NIST SP 800-76.

Control Objectives and Interoperability Requirements

[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.

The requirements of PIV-I are retained for PIV-II. Each agency's PIV implementation(s) shall meet the four control objectives (a) through (d) listed above.

[HSPD-12] also established requirements for Government-wide interoperability of identity credentials. These requirements, provided in paragraph 1 of the directive, are required in PIV-II and quoted here:

> (1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States 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 issued by the Federal Government to its employees and contractors (including contractor employees).

Each agency's PIV implementation(s) shall support interoperability by issuing and managing interoperable PIV Cards and their associated logical credentials specified in Section 4.

PIV Identity Proofing and Registration Requirements

Section 2.2 of this standard requires the adoption and use of an approved identity proofing and registration process. All PIV-II identity proofing and registration systems must satisfy the PIV-I objectives and requirements stated in Section 2.2 in order to be approved. 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.

An additional requirement for PIV-II is that the biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during the identity proofing and registration process.

When issuing PIV Cards, Federal agencies and departments must use an approved identity proofing and registration process. Two approved PIV identity proofing and registration processes are provided in Appendix A. Other identity proofing and registration process may be used if accredited by the department or agency as satisfying the requisite PIV objectives and requirements and approved in writing by the head of the Federal department or agency.

PIV Issuance and Maintenance Requirements

PIV Card Issuance

Section 2.3 of this standard requires the adoption and use of an approved issuance and maintenance process. All PIV-II issuance and maintenance systems must satisfy the PIV-I objectives and requirements stated in Sections 2.3 in order to be approved. An employee or contractor may be issued a PIV Card and logical credentials while a National Agency Check with Written Inquiries (NACI) or other OPM or National Security community investigation required for Federal employment is pending (see Section 2.2). In such cases, the process must verify successful completion and adjudication of the investigation.

An additional requirement is that the issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record. On successful match, the PIV Card shall be released to the applicant.

Two examples of PIV issuance process sets that satisfy the requisite PIV-II objectives and requirements are provided in Appendix A, Sections A.1.2 and Appendix A Sections A.2.2 through A.2.4. The heads of Federal departments and agencies may approve other identity proofing, registration, issuance process sets that are accredited as satisfying the requisite PIV-I objectives and requirements. Departments and agencies may enhance their issuance process to meet their local constraints and requirements.

PIV Card Maintenance

The PIV Card shall be maintained via processes that comply with the specifications in this section.

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 the employment is terminated, 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.

PIV Card Renewal

Renewal is the process by which a PIV Card is replaced without the need to repeat the full registration procedure. The card issuer shall 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 shall be followed in accordance with the OPM guidance.

The PIV Card shall be valid for no more than five years. A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card. 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.

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

shall be generated. If the PIV Card supports the optional key management key, it may be imported to the new PIV Card.

PIV Card Reissuance

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

A cardholder shall apply 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.

When these events are reported, normal operational procedures must be in place to ensure the following:

The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.

The CA shall 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. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers.

Online Certificate Status Protocol (OCSP) responders shall 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).

It is recommended that the old PIV Card, if available, is collected and destroyed. If the card cannot be collected, normal operational procedures shall complete 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.

PIV Card PIN Reset

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 shall 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 shall be formally documented by each department and agency.

PIV 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. The PIV Card shall 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 values must be updated to reflect the change in status.

The CA shall 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 shall include the appropriate certificate serial numbers.

OCSP responders shall 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 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.

Page 48: [2] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

[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. For conformance to this standard, PIV Card management systems are limited to algorithms and key sizes recognized by this standard and the current version of [COMMON].

Page 48: [3] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

Authority Information Access (AIA) extensions shall include pointers to the appropriate OCSP status responders, using the id-ad-ocsp access method as specified in Section 8 of [PROF], in addition to the Lightweight Directory Access Protocol (LDAP) Uniform Resource Identifiers (URI) required by [PROF].

If private key computations can be performed with the PIV authentication key without user intervention (beyond that required for cryptomodule activation), the corresponding certificate must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension.

Page 48: [4] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension, must include the PIV NACI indicator extension (see Appendix D), and must assert id-PIV-cardAuth in the extended key usage extension.

Page 48: [5] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

5: End Entity Signature Certificate Profile in [PROF], but shall not assert the nonRepudiation bit in the *keyUsage* extension, must include the PIV NACI indicator extension (see Appendix D), and must include the PIV Card's FASC-N in the subject alternative name field.

Page 59: [6] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

Section Break (Next Page)

PIV Processes

Sections 2.2 and 5.2 of this standard require the adoption and use an approved identity proofing and registration process. All identity proofing and registration systems must satisfy the PIV objectives and requirements stated in Sections 2.2 and 5.2 in order to be approved.

Section 2.3 and 5.3 of this standard requires the adoption and use of an approved credential issuance and management process. All credential issuance and management systems must satisfy the PIV objectives and requirements stated in Sections 2.3 and 5.3 in order to be approved. The heads of Federal departments and agencies may approve other identity proofing, registration and issuance process sets that are accredited as satisfying the requisite PIV objectives and requirements.

Two examples of PIV identity proofing, registration and issuance process sets that satisfy the requisite PIV control objectives and requirements are provided in this Appendix. Wherever appropriate, additional PIV-II requirements have been specified in order to meet the objectives of PIV-II.

Role Based Model

The role based identity proofing, registration and issuance process set is recommended for organizations not having a pre-existing PIV system.

PIV Identity Proofing and Registration

Departments and agencies that employ the generic process set for issuing PIV credentials shall follow the identity proofing and registration process defined in this section.

Roles and Responsibilities

The critical roles associated with the PIV identity proofing, registration and issuance process are defined below. These roles may be ancillary roles assigned to personnel who have other primary duties. The following roles shall be employed for identity proofing and issuance:

Applicant—The individual to whom a PIV credential needs to be issued.

PIV Sponsor—The individual who substantiates the need for a PIV credential to be issued to the Applicant, and provides sponsorship to the Applicant. The PIV Sponsor requests the issuance of a PIV credential to the Applicant.

PIV Registrar—The entity responsible for identity proofing of the Applicant and ensuring the successful completion of the background checks. The PIV Registrar provides the final approval for the issuance of a PIV credential to the Applicant.

PIV Issuer—The entity that performs credential personalization operations and issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The PIV Issuer is also responsible for maintaining records and controls for PIV credential stock to ensure that stock is only used to issue valid credentials.

PIV Digital Signatory—The entity that digitally signs the PIV biometrics and CHUID. This role only applies for PIV-II.

PIV Authentication Certification Authority (CA)—The CA that signs and issues the PIV Authentication Certificate. This role only applies to PIV-II.

The roles of PIV Applicant, Sponsor, Registrar, and Issuer are mutually exclusive; no individual shall hold more than one of these roles in the identity proofing and registration process. The PIV Issuer and PIV Digital Signatory roles may be assumed by one individual or entity. The PIV Authentication CA is a CA accredited to issue certificates under the Common Policy as specified in Section 5.4.1.

Individuals and entities assigned to the PIV Registrar, Issuer, or Digital Signatory roles shall meet the applicable requirements established by an official accreditation process.

Identity Proofing and Registration of New Employees and Contractors

An Applicant applies for a PIV credential as a part of the vetting process for Federal employment, or to seek access to Federally controlled physical facilities or information resources. This section of the document defines a process that uses identity source document inspection and background checks to establish assurance of identity. The process provides the minimal functional and security requirements for achieving a uniform level of assurance for PIV identity credentials; issuing organizations may enhance or expand upon the process to meet their organizational requirements as long as the resulting process meets the requirements set forth in this section. The identity proofing and registration requirements shall include the following:

The PIV Sponsor shall complete a PIV Request for a particular Applicant, and submit the PIV Request to the PIV Registrar and the PIV Issuer. The PIV Request shall include the following:

Name, organization, and contact information of the PIV Sponsor, including the address of the sponsoring organization

Name, date of birth, position, and contact information of the Applicant

Name and contact information of the designated PIV Registrar

Name and contact information of the designated PIV Issuer

Signature of the PIV Sponsor.

The PIV Registrar shall confirm the validity of the PIV Request prior to acceptance.

The Applicant shall complete Standard Form (SF) 85, OPM Questionnaire for Non-Sensitive Positions, or an equivalent, to provide the required background information. The Applicant shall then submit the completed background information form to the PIV Registrar.

The Applicant shall appear in person and provide two forms of identity source documents in original form to the PIV Registrar. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture identification (ID). The PIV Registrar shall visually inspect the identification documents and authenticate them as being genuine and unaltered. In addition, the PIV Registrar shall electronically verify the authenticity of the source document, when such services are offered by the issuer of the source document. When electronic verification is not offered, the PIV Registrar shall use other available tools to authenticate the source and integrity of the identity source documents. The PIV Registrar shall subsequently compare the picture on the source document with the Applicant to confirm that the Applicant is the holder of the identity source document. If all of the above checks are deemed to be successful, the PIV Registrar shall record the following types of data for each of the two identity source documents presented, sign the record, and keep it on file:

Document title

Document issuing authority

Document number

Document expiration date (if any)

Any other information used to confirm the identity of the Applicant.

The PIV Registrar shall compare the Applicant's information contained in the PIV Request (e.g., full name, date of birth, contact information) with the corresponding information provided by the Applicant.

The PIV Registrar shall capture a facial image of the Applicant and retain a file copy of the image. In PIV-II, if an electronic facial image is captured, it shall conform to the facial image specifications in [SP800-76].

The PIV Registrar shall fingerprint the Applicant, obtaining all the Applicant's fingerprints as defined in Section 4.4, and retain a copy. Additionally in PIV-II, two of the Applicant's fingerprints shall be collected in an electronic format compliant with Section 4.4.

The PIV Registrar shall initiate a National Agency Check with Inquiries (NACI) on the Applicant as required by Executive Order 10450 [EO10450]. Appendix C provides further detail on NACI and National Agency Check (NAC). Any unfavorable results of the investigation shall be adjudicated to determine the suitability of the Applicant for obtaining a PIV credential.

When all of the above requirements are completed, the PIV Registrar shall notify the Sponsor and the designated PIV Issuer that the Applicant has been approved for the issuance of a PIV credential. Conversely, if any of the required steps are unsuccessful, the PIV Registrar shall send appropriate notifications to the same authorities.

The PIV Registrar shall make available the following information to the PIV Issuer through a secure process:

Applicant's facial image

Copy of the results of the Applicant's background investigation

Other data associated with the Applicant (e.g., employee affiliation).

In PIV-II, the PIV Registrar shall make available the following information to the PIV Digital Signatory through a secure process:

Electronic biometric data for card personalization

Other data associated with the Applicant that is required for the generation of signed objects for card personalization.

The PIV Registrar shall be responsible for maintaining the following:

Completed and signed PIV Request

Completed and signed SF 85 (or equivalent) form received from the Applicant

Information related to the identity source documents checked

Results of the required background check

Copies of the facial image and fingerprints

Any other materials used to prove the identity of the Applicant.

All applicable Federal regulations for security, privacy, and records archival shall be followed in the implementation of the storage and access control mechanisms used to maintain the above data, including the privacy policies specified in Section 2.3.

Identity Proofing and Registration of Current Employees and Contractors

The identity proofing process described in Section A.1.1.2 shall be followed to issue or reissue PIV credentials to current employees and contractors. However, background checks are not required if the background check results can be referenced in the application process and verified by the PIV Registrar.

PIV Issuance

The PIV credential issuance process shall meet the functional and security requirements defined below. Departments and agencies may enhance the issuance process to meet their local constraints and requirements; however, the resulting process shall meet the requirements below.

The PIV Issuer shall confirm the validity of the PIV Request received from the Sponsor, and the approval notification received from the PIV Registrar. The PIV Issuer shall also confirm that the approval notification is consistent with the results of the background investigation.

The PIV Issuer shall control the creation and personalization of a new PIV credential using the information provided by the PIV Registrar. In PIV-II, the PIV Issuer shall initiate the creation of a CHUID for the new PIV credential. This CHUID shall be made available to the PIV Digital Signatory through a secure mechanism.

In PIV-II, the Digital Signatory shall create digitally signed credential elements (biometric and CHUID) needed for the card personalization process, using the data supplied by the PIV Registrar and the newly assigned CHUID. The digitally signed credential elements shall comply with the relevant specifications in Sections 4.2.2 and 4.4.2. The signed credential elements shall be made available to the PIV Issuer.

The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV credential. Before the newly created PIV credential is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:

The individual shall present a state or Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document matches the picture and name on the new PIV credential being personalized. Additionally, the PIV Issuer (or an authorized delegate) shall also validate that the appearance of the individual matches the picture being printed on the PIV credential.

In PIV-II, the PIV Issuer (or their authorized delegate) shall also check that the fingerprint of the individual matches the biometric credential embedded in the PIV credential.

In PIV-II, the Applicant may be asked to provide a PIN, or the PIV Issuer may generate a PIN on their behalf.

The PIV Issuer shall personalize the PIV credential. The personalized PIV credential shall meet all of the technical and interoperability specifications in Section 4 for compliance with PIV-II requirements.

In PIV-II, the Applicant may generate cryptographic key pair(s) for the PIV credential and obtain the corresponding certificates from the PIV Authentication CA at this time. Alternatively, the Applicant may be supplied a one-time authenticator[1] for use in a subsequent certificate request to the PIV Authentication CA. In the latter case, the Applicant will generate their key pair(s) at a local workstation[2] rather than at the PIV Issuer location.

In PIV-II, the recipient's name, issuer identity, card number, and possibly PKI certificate identification information shall be enrolled and registered with back-end data stores that support the PIV system. Depending on the infrastructure design, the back-end data stores may be centralized or decentralized.

The PIV Issuer (or an authorized delegate) shall obtain a signature from the Applicant (now PIV credential holder) attesting to the Applicant's acceptance of the PIV credential and the related responsibilities.

When all of the above requirements are completed, the PIV Issuer shall notify the PIV Sponsor and the designated PIV Registrar signifying that the personalization and issuance process has been completed. Conversely, if any of the required steps are unsuccessful, the PIV Registrar shall send appropriate notifications to the same authorities.

The PIV Issuer shall be responsible for maintaining the following:

Completed and formally authorized PIV Request

The approval notice from the PIV Registrar

The name of the PIV credential holder (Applicant)

The credential identifier. In PIV-II, this identifier is the Agency Card Serial Number

The expiration date of the PIV credential

The signed acceptance form from the PIV credential holder

All applicable Federal regulations for security, privacy, and records archival shall be followed in the implementation of the storage and access control mechanisms used to maintain the above data, including the privacy policies specified in Section 2.4.

System-Based Model

Organizations that possess an automated identity management system may choose to employ the system based identity proofing, registration and issuance process set. This section is provided by the Government Smart Card Interagency Advisory Board.

---

1 The issuing agency must ensure the necessary PKI management functions are supported and implemented in conformance with the security policy objectives mandated in [COMMON].

2 The issuing agency is responsible for the necessary PKI certificate management.

PIV Identity Proofing and Registration

For compliance to the PIV control objectives in Sections 2.2 and 5.2 of this standard, at a minimum, agencies employing the system-based identity proofing, registration and issuance process set using an Automated Identity Management System shall follow the identity proofing and registration process defined in Sections A.2.1- A.2.4 when issuing PIV credentials. Figure A-1, PIV Identity Verification and Issuance, shows the logical components that comprise a PIV identity proofing and credential issuance process. This diagram illustrates the minimum mandatory components and roles required to support PIV control objectives and requirements.

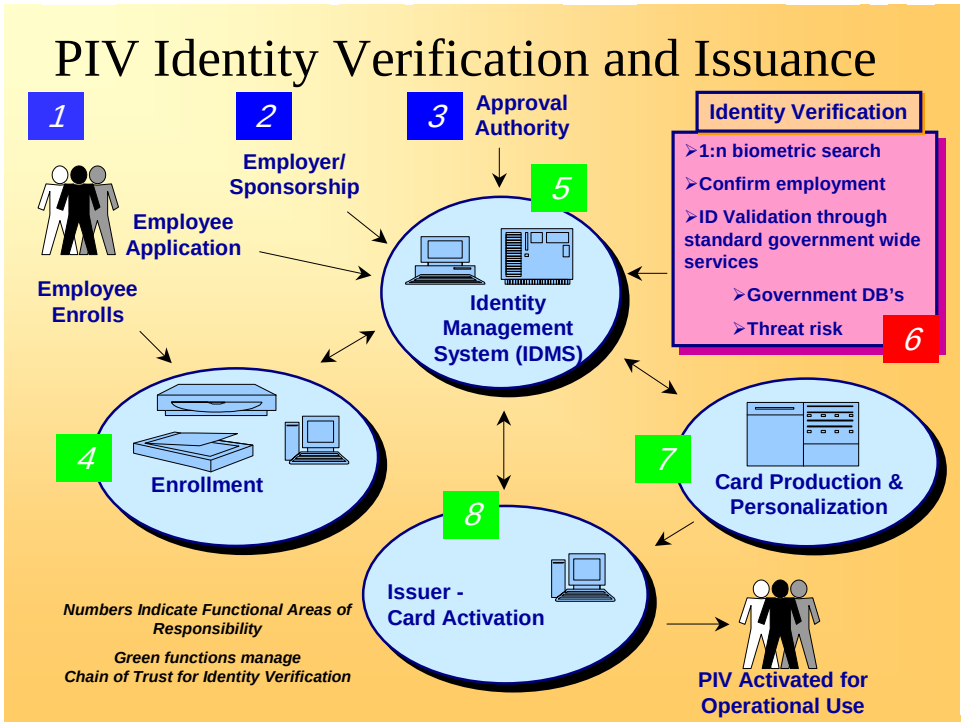


Figure A-1. PIV Identity Verification and Issuance

Roles and Responsibilities

The roles associated with the system-based PIV identity proofing, registration and issuance process are defined below:

Applicant—The individual to whom a PIV credential is to be issued. Individuals shall provide the necessary supporting identity-source documents to prove the claimed identity.

Employer/Sponsor— The individual who substantiates the relationship to the Applicant and provides sponsorship to Applicant. The employer/sponsor shall authorize the request for a PIV credential.

Enrollment Official— The individual who initiates the chain of trust for identity proofing and provides trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate the identity-source documentation. The Enrollment Official delivers a secured enrollment package to the IDMS for adjudication.

Approval Authority—The entity that establishes organizational chain of command within the Identity Management System (IDMS) for PIV application approvals. This includes establishing approved Employer/Sponsors. May designate automated or manual approval processes for completed PIV applications. Shall manage the total scope of the chain of trust established in functional process. Shall manage appropriate privacy and security controls.

Issuing Authority (Issuer) —The entity that issues the PIV credential to the Applicant after all identity proofing, background checks, and related approvals have been completed.

The issuer shall complete the chain of trust by performing 1:1 biometric check of the applicant against the PIV enrollment record. Upon confirmation of correct individual, the issuer shall activate the card. The issuer shall then release the credential to the individual.

Roles are not defined to mandate that a single individual within an organization must fulfill any given role. All roles and processes may be provided by accredited service providers compliant with this standard.

The Approval Authority shall practice best practices for separation of roles and responsibilities according to risk. The Approval Authority shall ensure the system has at least two persons performing different functions in the chain of trust processes. The principle of separation of duties shall be enforced to ensure that no single individual has the capability to issue a PIV credential without the participation of another authorized person. Card production may be accomplished either centrally or at a distributed issuer facility, provided security and quality control objectives for card stock management are fully met. The Applicant must appear in-person at least once before the issuance of a PIV card.

The components associated with the PIV identity proofing and issuance are:

Identity Management System—The Approval Authority shall maintain the IDMS that shall be the system of records for PIV credentials issued. It performs the identity proofing, verification and validation to establish identity claim validity. Shall provide a 1:many search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services (6) which shall be provided in accordance with HSPD-11. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.

Enrollment System—Initiates the chain of trust for identity proofing. Enrollment shall be provided trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.

Card Production and Personalization System—Shall provide full inventory controlled process to print and personalize PIV credentials per approval of the IDMS. Shall provide mechanisms to track status, control inventory, and protect blank card stock and personalized/printed card stock prior to activation.

PIV Identity Proofing and Issuance Requirements and Workflow are:

Applicant—The individual to whom an identity credential is to be issued. Individual shall provide supporting enrollment documentation for claimed identity.

Employers/Sponsors—Shall substantiate the relationship to the Applicant and provide sponsorship of Applicant. Shall authorize the request for a PIV credential.

Approval Authority—Is responsible for and shall manage the total scope of the chain of trust established in functional process areas 4 through 8 in *Figure A-2*.

Enrollment—Initiates the chain of trust for identity proofing. Enrollment shall provided trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.

Identity Management System—The Approval Authority shall maintain an IDMS that shall be the system of records for PIV credentials issued by that Approval Authority. The IDMS performs the identity proofing, verification and validation to establish identity claim validity. Shall provide a search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services (6) which shall be provided in accordance with HSPD-11. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.

Card Production and Personalization—Shall provide full inventory controlled process to print and personalize PIV credentials per approval of the IDMS. Shall provide mechanisms to protect blank card stock, consumable supplies, and personalized/printed card stock prior to activation.

Issuer—The entity that issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The issuer shall complete the chain of trust by: performing 1:1 biometric check of applicant against PIV enrollment record, verifying photograph in enrollment record matches the individual. Upon confirmation of correct individual, the issuer shall activate the card. Upon activation, the issuer shall close the chain of trust by having the individual verify their biometrics against the PIV credential. The issuer shall then release the credential to the individual.

Identity Proofing and Enrollment

All actions taken for approval/denial of requests by all participants in this process shall have an auditable trail that can support both forensic and system management capabilities. This audit trail shall provide a critical control component for the chain of trust for PIV issuance and management.

Employer/Sponsor

Employer/Sponsors must be pre-registered in the IDMS. The Approval Authority must establish roles for Employer/Sponsors. These may be government organizations or contractor organizations. The Approval Authority shall establish appropriate delegation of authority to Employer/Sponsors to approve PIV applications of Applicants.

PIV Application Process

The PIV Application Process has four components:

The Applicant request and claimed identity documentation,

The Employer/Sponsor approval of Applicant request,

The approval authority confirms and approves PIV application, appropriate sponsorship, and shall approve the PIV request,

The enrollment to bind the submissions from (1), (2) and (3) for formal submission to the IDMS initiating the identity verification and validation process.

The Applicant shall provide a formal request for a PIV.

The Employer/Sponsor shall approve the Applicant request.

Once the Applicant has gained the sponsorship and approval of the Employer, the Applicant shall appear for Enrollment. The Applicant shall provide a minimum of two forms of identification from the list of acceptable documents included in the *Form 1-9, OMB No. 1115-0136, Employment Eligibility Verification* to the PIV Registration Authority. At least one of the documents shall be a valid State or Federal Government-issued picture ID.

PIV Enrollment Process

The PIV Enrollment process shall provide the following minimum steps:

Applicant shall appear for enrollment with supporting documentation;

Enrollment shall inspect and confirm all supporting documents using automated means if available;

Enrollment shall establish that the individual present matches the supporting documents;

Enrollment shall confirm Employer/Sponsor approval for PIV; and

Enrollment shall scan all supporting documents.

The PIV Binding process shall provide the following minimum steps:

Enrollment shall take biometric samples and photograph of the Applicant;

Enrollment shall manage the quality assurance process of the biometric and photographic capture. The biometric samples shall be verified to ensure proper performance; and

Enrollment shall bind the completed electronic enrollment package with a digital signature and forward the enrollment application to the IDMS for identity verification and validation.

The completed PIV enrollment package shall include:

Scanned documents supporting identity claim;

Biometric samples and digital photograph;

Personal biographic and organizational information; and

Digital signature of Enrollment Official.

Identity Verification Process

The IDMS shall receive the completed package for PIV from Enrollment. The IDMS shall verify the integrity of that package by confirming completeness, accuracy, and digital signatures.

The IDMS shall provide a means to confirm employment and sponsorship as identified in the package.

The IDMS shall perform a 1:many search to assure that the individual identified in the package has not applied previously under a different name.

The IDMS shall conduct the appropriate identity verification and validation using government-wide databases and services in accordance with HSPD-11.

The Approval Authority shall provide adjudication of identity claim should any of these three core checks identify a potential risk.

After successful completion of the appropriate identity verification process, the Approval Authority shall approve card production for the credential. The Approval Authority may approve issuance of a PIV credential prior to completion of all core checks for identity verification and validation if these processes exceed ten days.

The IDMS shall be responsible to maintain:

Completed and signed PIV enrollment package;

Copies of the identity source documents;

Completed and signed background form received from the Applicant;

Results of the required background check;

Any other materials used to prove the identity of the Applicant;

The credential identifier such as an identity credential serial number;

The expiration date of the identity credential;

Unique minimal identity record for each approved Applicant;

Separated database indexed to the minimal identity record containing the original biometric data captured at enrollment. These data shall be encrypted at rest; and

Separated database of biometric data indexed to the minimal identity record supporting AFIS for 1:many identity checking.

The IDMS shall provide services that:

Notify the Employee/Contractor Applicant of status of the PIV;

Notify the Employer of status of the PIV; and

Enable validation by anyone inquiring if an issued credential is still valid.

The IDMS shall provide complete personalization and printing information for card production for all approved PIV credentials as required by the supporting card production facility's requirements. This information shall be provided to enable the full chain of trust between the individual, the issuer, the identity verification performed, the credential and the biometric.

Card Production, Activation and Issuance

Card production may be performed either centrally or in a distributed location. The IDMS shall track the status of a PIV credential throughout its life cycle, from initial production request, personalization and printing, activation and issuance, suspension, revocation and destruction.

Card production services shall—

Maintain full inventory control of blank initialized or pre-issued (e.g. with the manufacturers keys) stock, consumables and manufacturing materials;

Maintain a list of approved IDMS systems that can submit PIV requests for card production,

Provide acknowledgement of IDMS request to produce a PIV;

Notify the IDMS upon completion of PIV credential production;

Maintain a list of approved Issuers that can activate and issue PIV credentials;

Only send information regarding production of PIV credentials to approved authorities;

Only send fully completed and personalized PIV credentials to approved Issuing Agents; and

Document, implement, and maintain a Card Production, Activation and Issuance Security Policy.

At time of activation, the Issuer shall establish that the individual seeking to activate their PIV credential is the individual who applied for the PIV with a 1:1 biometric verification to the IDMS. Once confirmed, the Issuer shall activate the credential.

Suspension, Revocation and Destruction

It is important to keep track of active cards as well as lost, stolen and expired cards. A card registry for all cards issued shall be established and maintained.

Re-issuance to Current PIV Credential Holders

When issuing or re-issuing identity credentials to current employees, the Issuing Authority shall—

Insure the IDMS record for this individual states the credential is not expired;

Verify the individual with a 1:1 biometric match against the IDMS record;

Verify the individual against the IDMS record digital photograph;

Recapture biometrics;

Issue a new credential and update the IDMS record; and

The recaptured biometrics and new credential record shall be digitally signed by the Issuing Authority.

Page 61: [7] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

NIST plans to develop a PIV validation program that will test implementations for conformance with this standard. Note that the following is not requirements until NIST establishes a program. Information on this program will be published at as it becomes available.

A PIV system is FIPS 201-compliant after each of its constituent components (card, reader, issuer software, and registration database) has met its individual validation requirements. Because these individual validation requirements are based on different standards and no single test laboratory is accredited for validating products built to all these standards, a PIV system has to undergo testing and consequent validation through multiple validation facilities. The PIV components and currently available validation requirements are summarized in Table B-1.

Table B-1. PIV System Components and Validation Requirements

PIV Component	Validation Requirement(s)
PIV ICC	ISO/IEC 7816, ISO/IEC 10373 (Parts 1 and 3) ISO/IEC 14443 (Parts 1-4), ISO/IEC 10373 (Part 6) Crypto Modules—FIPS 140-2
PIV Reader	PC/SC
Card Issuance and Maintenance System	Crypto Modules—FIPS 140-2

Page 66: [8] Deleted **FIPS201-2 changes** **3/1/2011 1:15:00 PM**

Physical Access Control Mechanisms

The Government Smart Card Interagency Advisory Board's Physical Security Interagency Interoperability Working Group publication *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems* (PACS) provides guidance on physical access for various assurance profiles. Table C-1 describes the relationship between the PACS assurance levels and the PIV identity authentication levels defined in Section 6.1.

Table E-1. PIV Support of PACS Assurance Profiles

PACS Assurance Profile	PIV Identity Authentication Assurance Levels
PACS Low	SOME confidence
PACS Medium	SOME confidence
PACS High (without PIN)	SOME confidence
PACS High (with PIN)	VERY HIGH confidence

Section Break (Next Page)

6/23/06	D.2, Pg. 68	Delete “DEFAULT FALSE” to the ASN.1 module for the NACI indicator extension and replace underscores with dashes as follows: PIV-Cert-Extensions { 2 16 840 1 101 3 6 10 1 } DEFINITIONS EXPLICIT TAGS ::= BEGIN -- EXPORTS ALL -- -- IMPORTS NONE -- Id-piv-NACI OBJECT IDENTIFIER ::= { 2 16 840 1 101 3 6 9 1 } NACI-indicator ::= BOOLEAN END