FIPS PUB 201

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

Personal Identity Verification (PIV) of Federal Employees and Contractors

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

February 25, 2005

U.S. DEPARTMENT OF COMMERCE
Carlos M. Gutierrez, Secretary

TECHNOLOGY ADMINISTRATION
Phillip J. Bond, Under Secretary for Technology

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Hratch G. Semerjian, Acting Director

Acknowledgements

NIST would like to acknowledge the significant contributions of the Federal Identity Credentialing Committee (FICC) 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 workshops and provided valuable technical suggestions in shaping this standard. NIST also acknowledges the comments received from government and industry organizations during the FIPS 201 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.

Dr. Shashi Phoha, Director
Information Technology Laboratory

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 two major sections. Part one describes the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive 12, including personal identity proofing, registration, and issuance. Part two 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. Similarly, the interfaces and data formats of biometric information are specified in Special Publication 800-76, Biometric Data Specification for Personal Identity Verification.

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

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
2005

Announcing the
Standard for

Personal Identity Verification
of
Federal Employees and Contractors

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: Personal Identity Verification (PIV) of Federal Employees and Contractors.

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.

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, this 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 consists of two parts—PIV-I and PIV-II. PIV-I satisfies the control objectives and meets the security requirements of HSPD 12, while PIV-II meets the technical interoperability requirements of HSPD 12. PIV-II specifies implementation and use of identity credentials on integrated circuit cards for use in a Federal personal identity verification system.

PIV Cards 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 may self-accredit, or use other accredited issuers, to issue identity credentials for Federal employees and contractors until a government-wide PIV-II accreditation process is established. The standard also covers security and interoperability requirements for PIV Cards. Funding permitting, NIST plans to develop a PIV Validation Program that will test implementations for conformance with this standard. Additional information on this program will be published at http://csrc.nist.gov/PIV-Project/Conformance/ as it becomes available.

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

9. Effective Date.

This standard is effective immediately. Federal departments and agencies shall meet the requirements of PIV-I no later than October 27, 2005, in accordance with the timetable specified in HSPD 12. The OMB has advised NIST that it plans to issue guidance regarding the transition from PIV-I to PIV-II. It is anticipated that some Federal departments and 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 will review this standard within five years to assess its adequacy. 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/.

Table of Contents

1. Introduction 1

1.1 Purpose 1
1.2 Scope 1
1.3 Document Organization 2

2. Common Identification, Security, and Privacy Requirements 5

2.1 Control Objectives 5
2.2 PIV Identity Proofing and Registration Requirements 5
2.3 PIV Issuance and Maintenance Requirements 6
2.4 PIV Privacy Requirements 7

3. PIV System Overview 10

3.1 Functional Components 10
3.1.1 PIV Front-End Subsystem 11
3.1.2 PIV Card Issuance and Management Subsystem 12
3.1.3 Access Control Subsystem 12
3.2 PIV Card Life Cycle Activities 13

4. PIV Front-End Subsystem 15

4.1 Physical PIV Card Topology 15
4.1.1 Printed Material 15
4.1.2 Tamper Proofing and Resistance 15
4.1.3 Physical Characteristics and Durability 16
4.1.4 Visual Card Topography 17
4.1.5 Logical Credentials 29
4.1.6 PIV Card Activation 29
4.2 Cardholder Unique Identifier (CHUID) 30
4.2.1 PIV CHUID Data Elements 30
4.2.2 Asymmetric Signature Field in CHUID 30
4.3 Cryptographic Specifications 31
4.4 Biometric Data Specifications 33
4.4.1 Biometric Data Collection, Storage, and Usage 34
4.4.2 Biometric Data Representation and Protection 35
4.4.3 Biometric Data Content 36
4.5 Card Reader Specifications 36
4.5.1 Contact Reader Specifications 37
4.5.2 Contactless Reader Specifications 37
4.5.3 PIN Input Device Specifications 37

5. PIV Card Issuance and Management Subsystem 38

5.1 Control Objectives and Interoperability Requirements 38
5.2 PIV Identity Proofing and Registration Requirements 38
5.3 PIV Issuance and Maintenance Requirements 39
5.3.1 PIV Card Issuance 39
5.3.2 PIV Card Maintenance 39
5.4 PIV Key Management Requirements 41
5.4.1 Architecture 41
5.4.2 PKI Certificate 41

5.4.3 X.509 CRL Contents 43
5.4.4 Migration from Legacy PKIs 43
5.4.5 PKI Repository and OCSP Responder(s) 43
5.5 PIV Privacy Requirements 44

6. PIV Card Authentication 45

6.1 Identity Authentication Assurance Levels 45
6.1.1 Relationship to OMB's E-Authentication Guidance 45
6.2 PIV Card Authentication Mechanisms 46
6.2.1 Authentication Using PIV Visual Credentials (VIS) 46
6.2.2 Authentication Using the PIV CHUID 47
6.2.3 Authentication Using PIV Biometric 48
6.2.4 Authentication Using PIV Asymmetric Cryptography (PKI) 49
6.3 PIV Support of Graduated Assurance Levels for Identity Authentication 50
6.3.1 Physical Access 50
6.3.2 Logical Access 51

List of Appendices

Appendix A— PIV Processes 52

A.1 Role Based Model 52
A.1.1 PIV Identity Proofing and Registration 52
A.1.2 PIV Issuance 55
A.2 System-Based Model 57
A.2.1 PIV Identity Proofing and Registration 57
A.2.2 Card Production, Activation and Issuance 62
A.2.3 Suspension, Revocation and Destruction 62
A.2.4 Re-issuance to Current PIV Credential Holders 62

Appendix B— PIV Validation, Certification, and Accreditation 64

B.1 Accreditation of PIV Service Providers 64
B.2 Security Certification and Accreditation of IT System(s) 64
B.3 Conformance of PIV Components to this Standard 64
B.4 Cryptographic Testing and Validation (FIPS 140-2 and algorithm standards) 64

Appendix C— Background Check Descriptions 66

Appendix D— PIV Object Identifiers 67

Appendix E— Physical Access Control Mechanisms 68

Appendix F— Glossary of Terms, Acronyms, and Notations 69

F.1 Glossary of Terms 69
F.2 Acronyms 73
F.3 Notations 75

Appendix G— References 76

List of Figures

Figure 3-1. PIV System Notional Model 11
Figure 3-2. PIV Card Life Cycle Activities 13
Figure 4-1. Card Front—Printable Areas 21
Figure 4-2. Card Front—Optional Data Placement—Example 1 22
Figure 4-3. Card Front—Optional Data Placement—Example 2 23
Figure 4-4. Card Front—Optional Data Placement—Example 3 24
Figure 4-5. Card Front—Optional Data Placement—Example 4 25
Figure 4-6. Card Back—Printable Areas and Required Data 26
Figure 4-7. Card Back—Optional Data Placement—Example 1 27
Figure 4-8. Card Back—Optional Data Placement—Example 2 28
Figure A-1. PIV Identity Verification and Issuance 57

List of Tables

Table 6-1. Relationship Between PIV and E-Authentication Assurance Levels 46
Table 6-2. Authentication for Physical Access 51
Table 6-3. Authentication for Logical Access 51
Table B-1. PIV System Components and Validation Requirements 64
Table D-1. PIV Object Identifiers 67
Table E-1. PIV Support of PACS Assurance Profiles 68

[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 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 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 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 identification 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.

1.1 Purpose

This standard defines a reliable, government-wide PIV system 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.

This standard specifies a PIV system within which common identification credentials 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.

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 identification 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 identification credential. In accordance with HSPD 12, this standard defines the technical requirements for the identity credential 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.

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. Access authorization decisions are outside the scope of this standard.

1.3 Document Organization

This standard is composed of two parts, PIV-I and PIV-II. The first part (PIV-I) describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of HSPD 12, including personal identity proofing, registration, and issuance, but does not address the interoperability of PIV Cards and systems among departments and agencies.

The second part (PIV-II) provides detailed technical specifications to support the control and security objectives in PIV-I as well as interoperability among Federal departments and agencies. PIV-II describes the policies and minimum requirements of a PIV Card that allows interoperability of credentials for physical access 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.

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 PIV-I, by establishing the control and security objectives for compliance with HSPD 12.

+ Section 3, PIV System Overview, serves to provide a PIV system overview. This section is *informative*.

+ 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.

+ Section 5, PIV Card Issuance and Management Subsystem, defines the components and processes that are part of the PIV-II. It also provides the requirements and specifications related to this subsystem.

+ Section 6, PIV Card 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.

+ Appendix A, PIV Processes, provides two models for identity proofing, registration, issuance, and maintenance of identity credentials. This section is *informative*.

+ Appendix B, PIV Validation, Certification, and Accreditation, provides guidance for the compliance with this document.

+ Appendix C, Background Check Descriptions, provides the requirements for background checks. This section is *informative*.

+ Appendix D, PIV Object Identifiers, provides additional details for the PIV objects identified in Section 4.

+ Appendix E, 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, Glossary of Terms and Acronyms, describes the vocabulary and textual representations used in the document. This section is *informative*.

+ Appendix G, References, lists the specifications and standards referred to in this document. This section is *informative*.

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 six months following promulgation of the standard.

2. Common Identification, Security, and Privacy Requirements

This section provides the requirements for the first part of the standard. PIV-I addresses the fundamental control and security objectives outlined in HSPD 12, including the personal identity proofing process for employees and contractors. 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;
+ 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 valid Federal or State government issued picture ID;
+ Fraudulent identity source documents are not accepted as genuine and unaltered;
+ A person suspected or known to the government as being a terrorist is not issued a credential;
+ No substitution occurs in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, is the person to whom the credential is issued;
+ No credential is issued unless requested by proper authority;
+ A credential remains serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked;
+ A single corrupt official in the process may not issue a credential with an incorrect identity or to a person not entitled to the credential;
+ An issued credential is not modified, duplicated, or forged;

2.2 PIV Identity Proofing and Registration Requirements

For compliance with the PIV-I control objectives, departments and agencies shall follow an identity proofing and registration process that meets the requirements defined below when issuing identity credentials.

+ The organization shall adopt and use an approved identity proofing and registration process.

+ The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. At a minimum, the National Agency Check (NAC) shall be completed before credential issuance.[1] Appendix C, Background Check Descriptions, provides further details on NAC and NACI.

+ The applicant must 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 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 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.

The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency Inspector General as satisfying the requirements above and approved in writing by the head of the Federal department or agency. Two examples of processes that meet these requirements are provided in Appendix A, PIV Processes.

These 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.

2.3 PIV Issuance and Maintenance Requirements

For compliance with the PIV-I control objectives, departments and agencies shall meet the requirements defined below when issuing identity credentials. The issuance and maintenance 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. Two examples of processes that meet these requirements are provided in Appendix A.

+ The organization shall use an approved PIV credential issuance and maintenance process.

+ The process shall ensure completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (NACI), or other OPM or National Security community investigation as required for Federal employment. The PIV credential shall be revoked if the results of the investigation so justify.

+ At the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.

[1] Note: a completed National Agency Check is sufficient for credential issuance; however, the required National Agency Check with Inquiries must still be completed.

+ 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).

2.4 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 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 may not assume any other operational role in the PIV system.

+ Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with [E-Gov] and [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, personal information in identifiable form [IIF]), 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. PIV applicants shall be provided full disclosure of the intended users of the PIV credential and the related privacy implications.

+ Assure that systems that contain IIF 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 IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.

+ Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.

+ Assure that the technologies used in the department or agency's implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.

+ Utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable. [SP800-53]

+ 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 credential.

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.

3. PIV System Overview

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

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.

+ **Access Control Subsystem**—the physical and logical access control systems, the protected resources, and the authorization data.

The access control 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 discussed in Section 6 to provide consistent and secure means for performing the authentication function preceding an access control decision.

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.

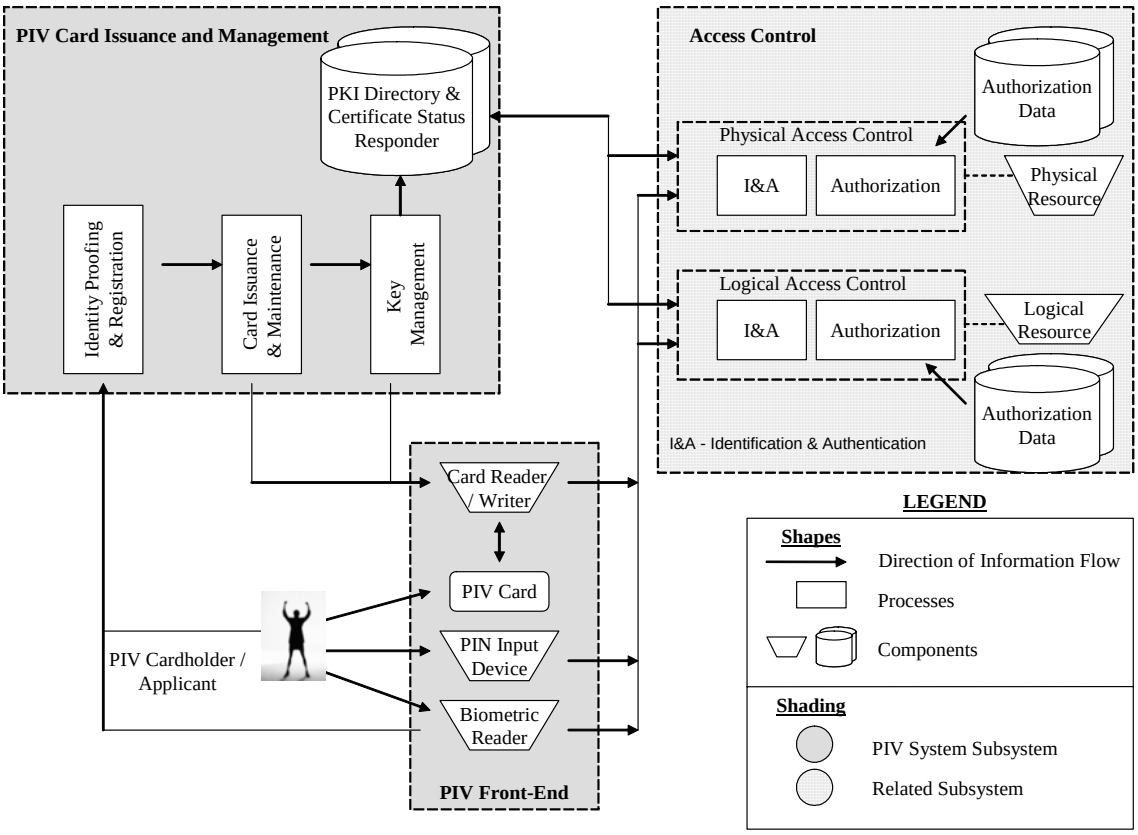


Figure 3-1. PIV System Notional Model

3.1.1 PIV Front-End Subsystem

The PIV Card will be issued to the applicant when all registration 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, 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").[2]

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.

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 not only printing photographs, names, and other information on the card, but also loading the relevant card applications, biometrics, and other data. 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 key 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.

3.1.3 Access Control Subsystem

The access control 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 entrance, room, turnstile, parking gate) that the cardholder wishes to access. The logical resource is typically a network or a location on the network (e.g., computer workstation, folder, file, database record, software program) to which the cardholder wants to gain access.

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

The physical and logical access control system grants or denies access to a particular resource and includes an identification and authentication (I&A) component as well as an authorization component. The I&A component interacts with the PIV Card and uses mechanisms discussed in Section 6 to identify

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

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

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.

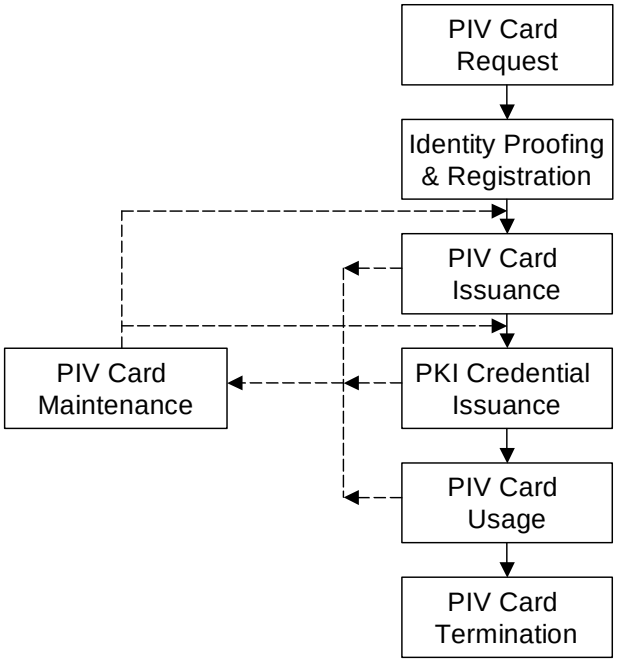


Figure 3-2. PIV Card Life Cycle Activities

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 PIV authentication so as to prevent any future use of the card for PIV authentication.

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 reader specifications.

4.1 Physical PIV Card Topology

References to the PIV Card in this section and Sections 4.1.1 through 4.1.4 pertain to the physical and physical topology 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.

Sections 4.1.1 through 4.1.4 contain information related to the physical topology of the PIV Card. The PIV Card's physical topology, appearance, and other characteristics should balance the need to have the PIV Card commonly recognized as a Federal identification card while providing the flexibility to support individual department and agency requirements. Having a common look for PIV Cards is important in meeting the objectives of improved security and interoperability. In support of these objectives, consistent placement of printed components and technology is generally necessary.

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

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 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 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.

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.
+ Departments and agencies may choose to punch an opening in the card body to enable the card 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 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.

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 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.

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 4.1.5.

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, as do constraints that prohibit printing over the embedded contactless module. The PIV Card topology provides flexibility for placement of the embedded module, either in the upper right-hand corner or in the lower bottom portion. Printing restrictions apply only to the area where the embedded module is located (i.e., upper right-hand corner, lower bottom portion).

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

4.1.4.1 Mandatory Items on the Front of the PIV Card

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

Zone 2—Name. The full name[3] shall be printed directly under the photograph in capital letters. The font shall be a minimum of 10 point.

Zone 8—Employee Affiliation. A printed employee affiliation shall be printed on the card. Some examples of employee affiliation are "CONTRACTOR," "ACTIVE DUTY," and "CIVILIAN."

Zone 10— Organizational Affiliation. The Organizational Affiliation shall be printed as depicted in Figure 4-1.

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

4.1.4.2 Mandatory Items on the Back of the Card

Zone 1—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 2—Issuer Identification. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.

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 3—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 topology space constraints, placement of a signature may limit the size of the optional two-dimensional bar code.

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

Zone 5—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 6—Portable Data File (PDF) Two-Dimensional Bar Code. If used, the PDF bar code placement shall be as depicted in the diagram (i.e., left side of the card). If Zone 3 (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 9— 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.

[3] Alternatively, pseudonyms as provided under the law.

Zone 11—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 12—Footer. The footer is the preferred location for the *Emergency Response Official Identification* label. If used, a department or agency may print "Federal Emergency Response Official" as depicted in Figure 4-2, preferably in red text. Departments and agencies may also print a secondary line in Zone 9 to further identify the Federal emergency respondent's official role. Some examples of official roles are "Law Enforcement, "Firefighter" and "Emergency Response Team (ERT)".

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

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

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

These colors shall be reserved and shall not be employed for other purposes. Zone 15 may be a solid or patterned line at the department or agency's discretion.

Zone 16—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 Zone 15 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 17—Agency Specific Data. In cases in which other defined optional elements are not used, Zone 17 may be used for other department or agency-specific information, as depicted in Figure 4-5.

4.1.4.4 Optional Items on the Back of the Card

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

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

Zone 5—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.

Zone 6—Additional Language for Emergency Responder 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 7—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 8—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 module selected. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.

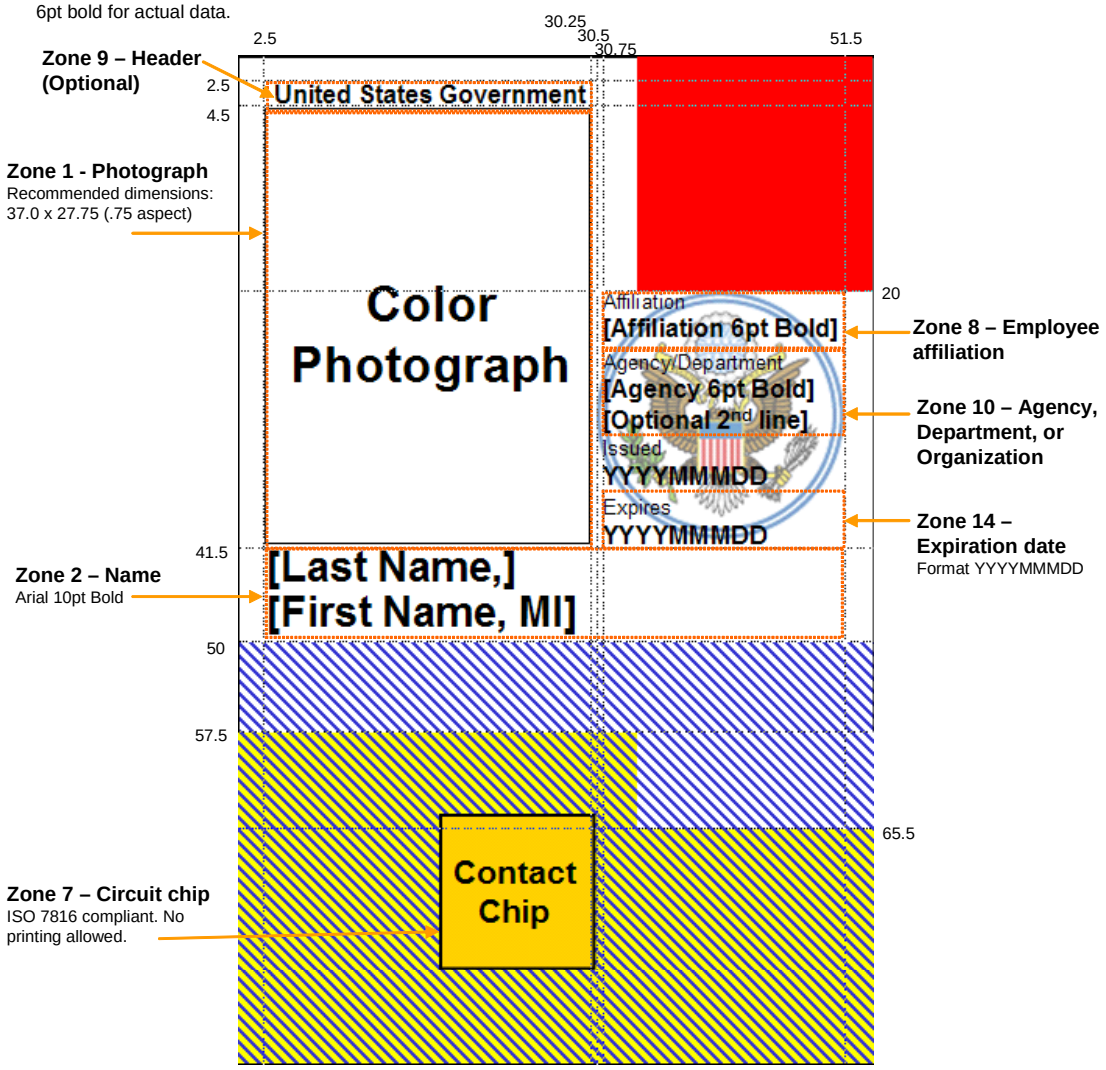
Zone 9—Agency-Specific Text. In cases in which other defined optional elements are not used, Zone 9 may be used for other department or agency-specific information, as depicted in Figure 4-8. For example, emergency responder officials may use this area to provide additional details.

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

For Zones 9 and 10, 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 medical entitlements that are legislatively mandated.

- 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 recommended font size is 5pt normal weight for data labels (also referred to as tags) and 6pt bold for actual data.



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. Note: In this example, Zone 9,11, and 13 are optional but shall be placed as depicted and therefore are not in the blue shaded area.

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.

Reserved area. No printing is permitted in this area unless verified as printable area by card and/or printer manufactuers.

Figure 4-1. Card Front—Printable Areas

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 recommended font size is 5pt normal weight for tags and 6pt bold for data.

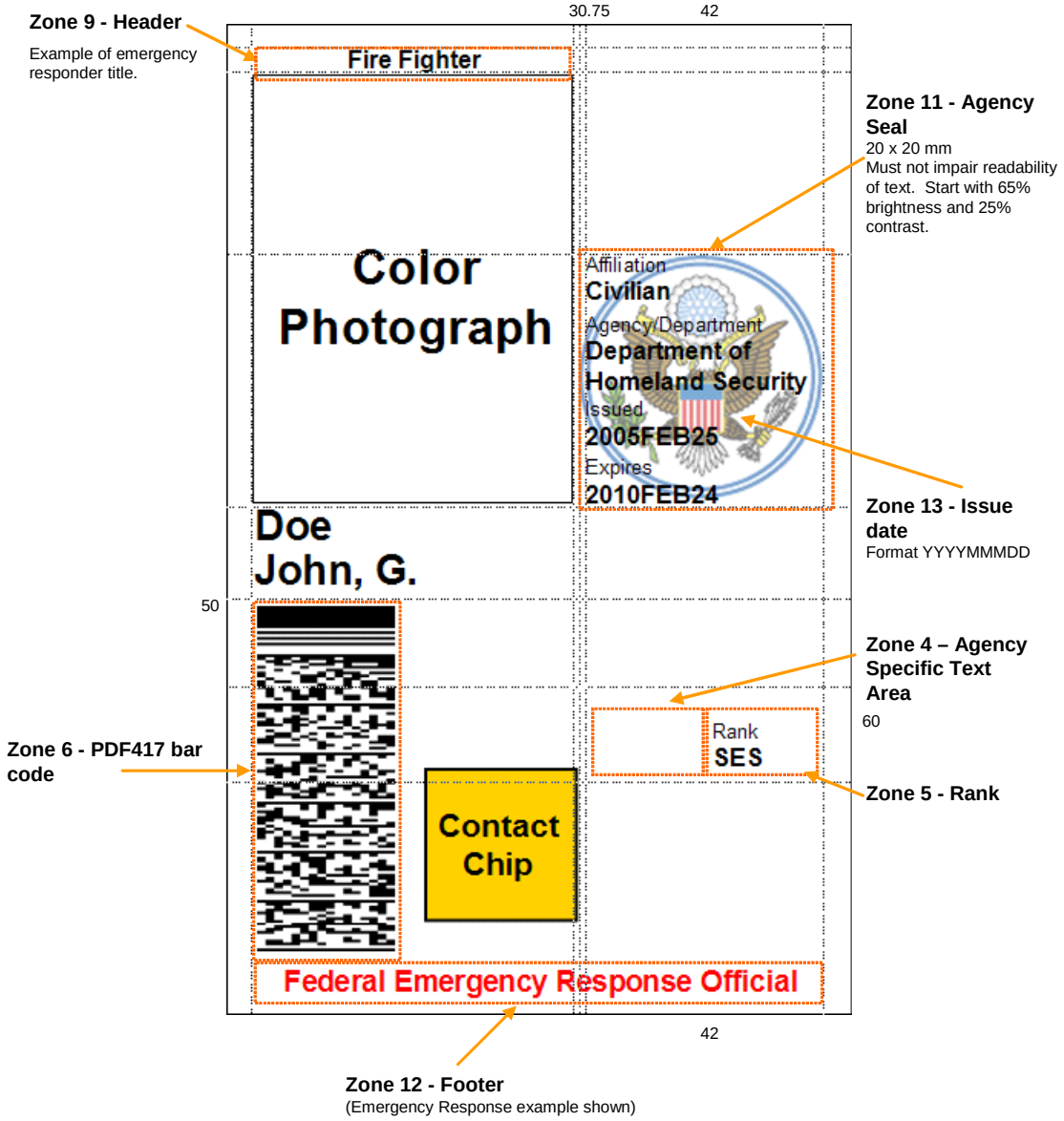


Figure 4-2. Card Front—Optional Data Placement—Example 1

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 recommended font size is 5pt normal weight for tags and 6pt bold for data.

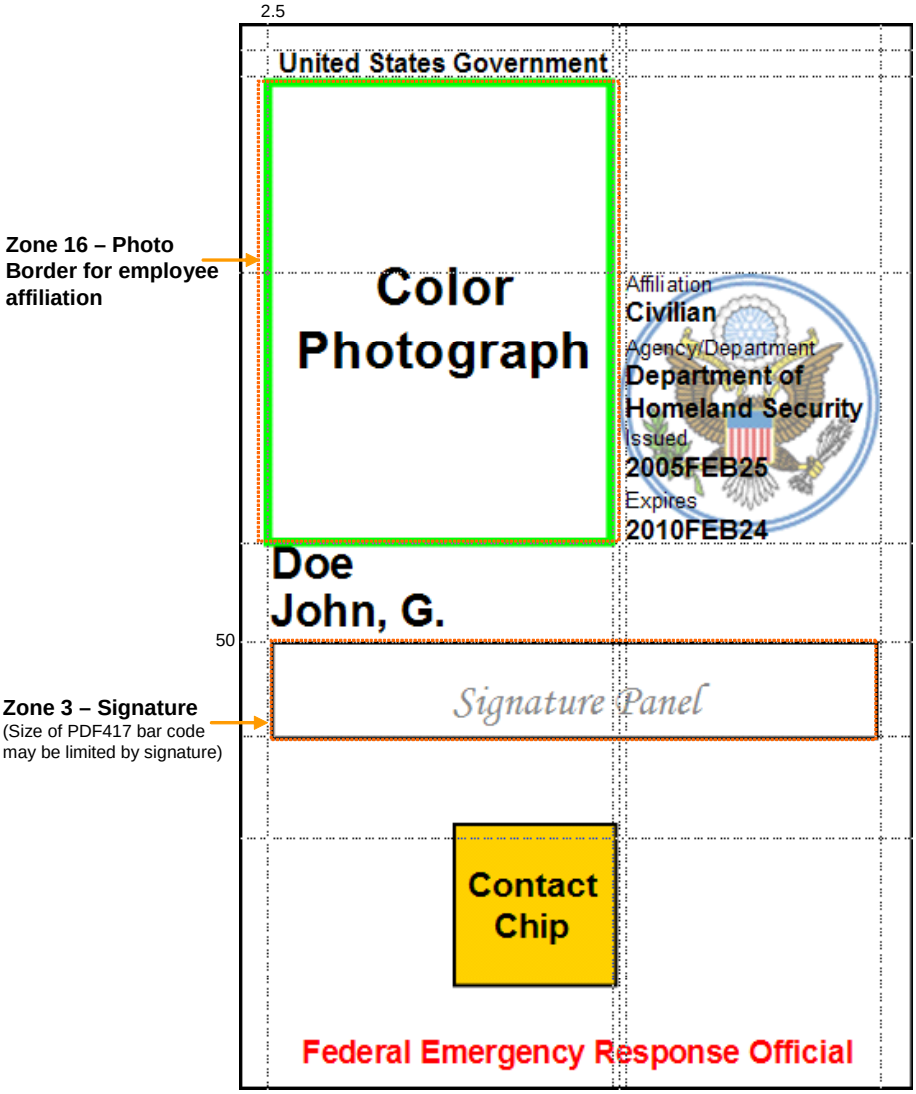


Figure 4-3. Card Front—Optional Data Placement—Example 2

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 recommended font size is 5pt normal weight for tags and 6pt bold for data.

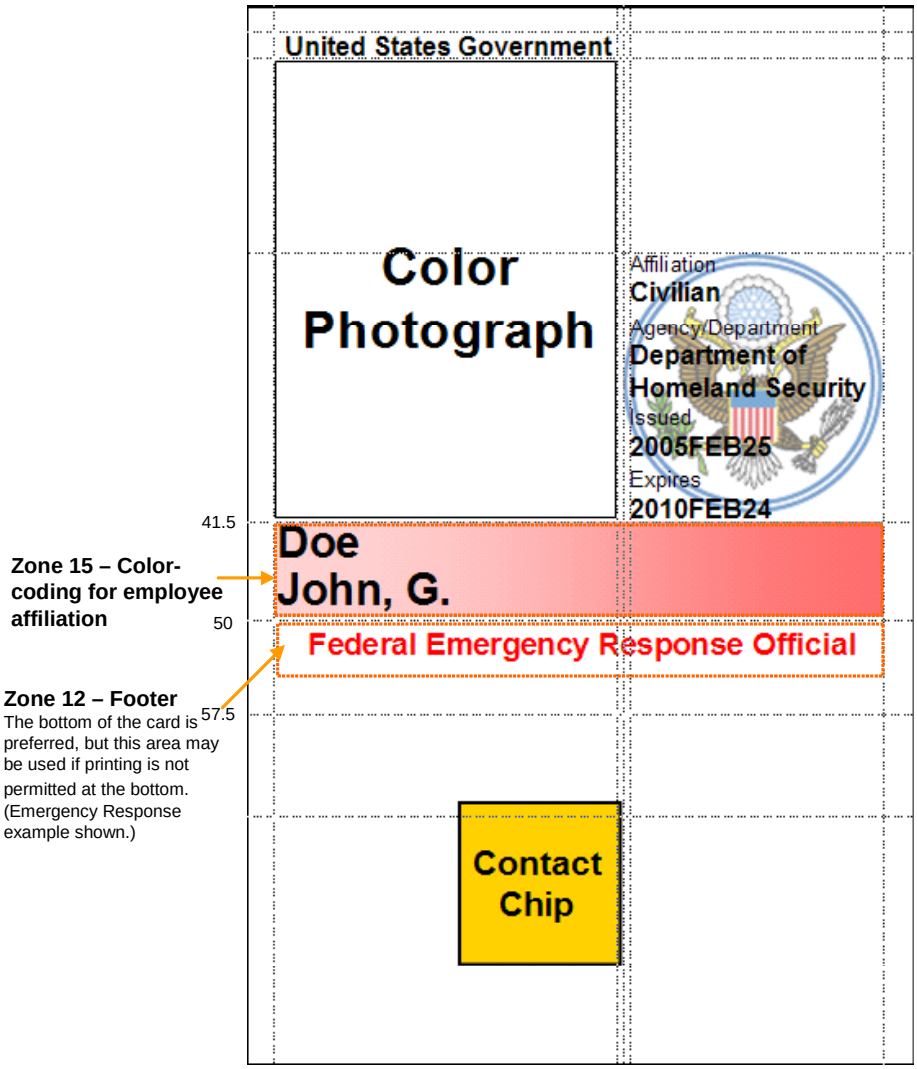


Figure 4-4. Card Front—Optional Data Placement—Example 3

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 recommended font size is 5pt normal weight for tags and 6pt bold for data.

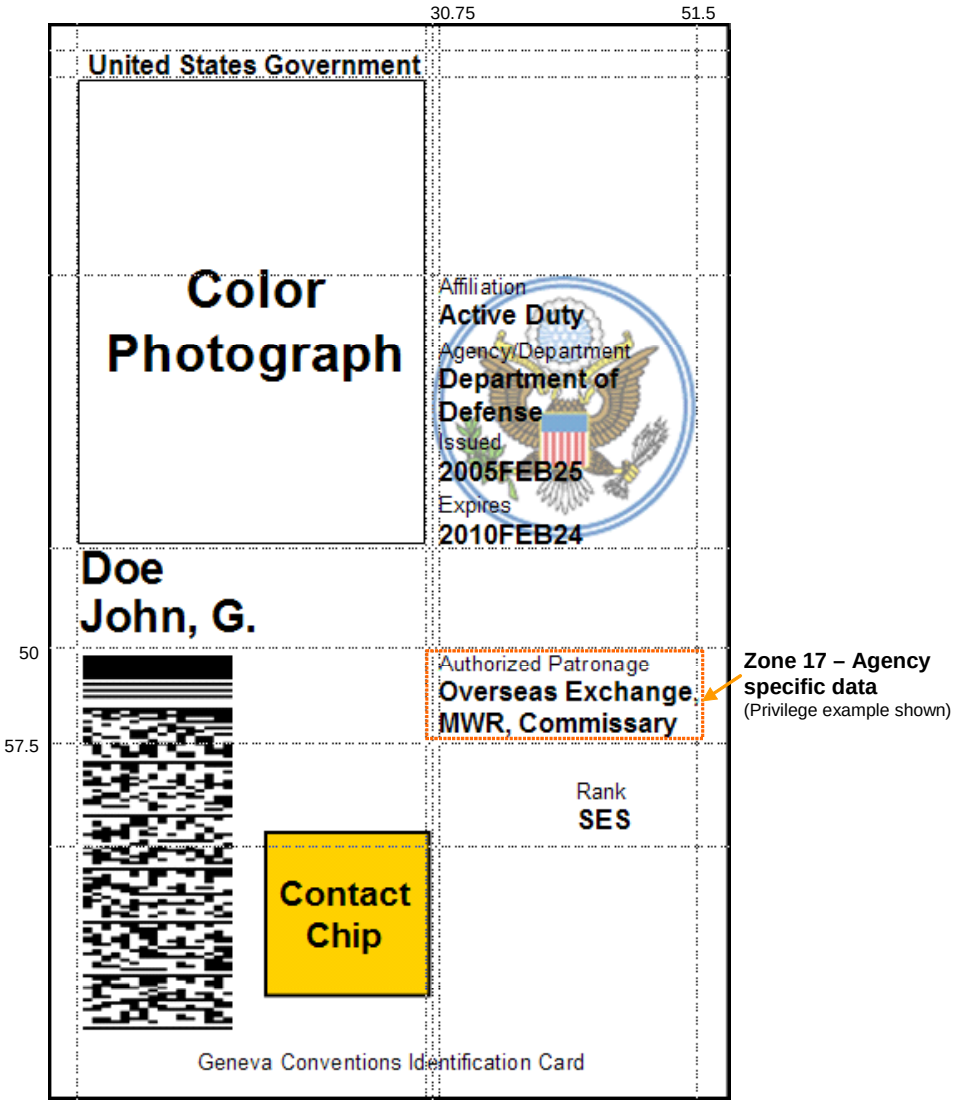
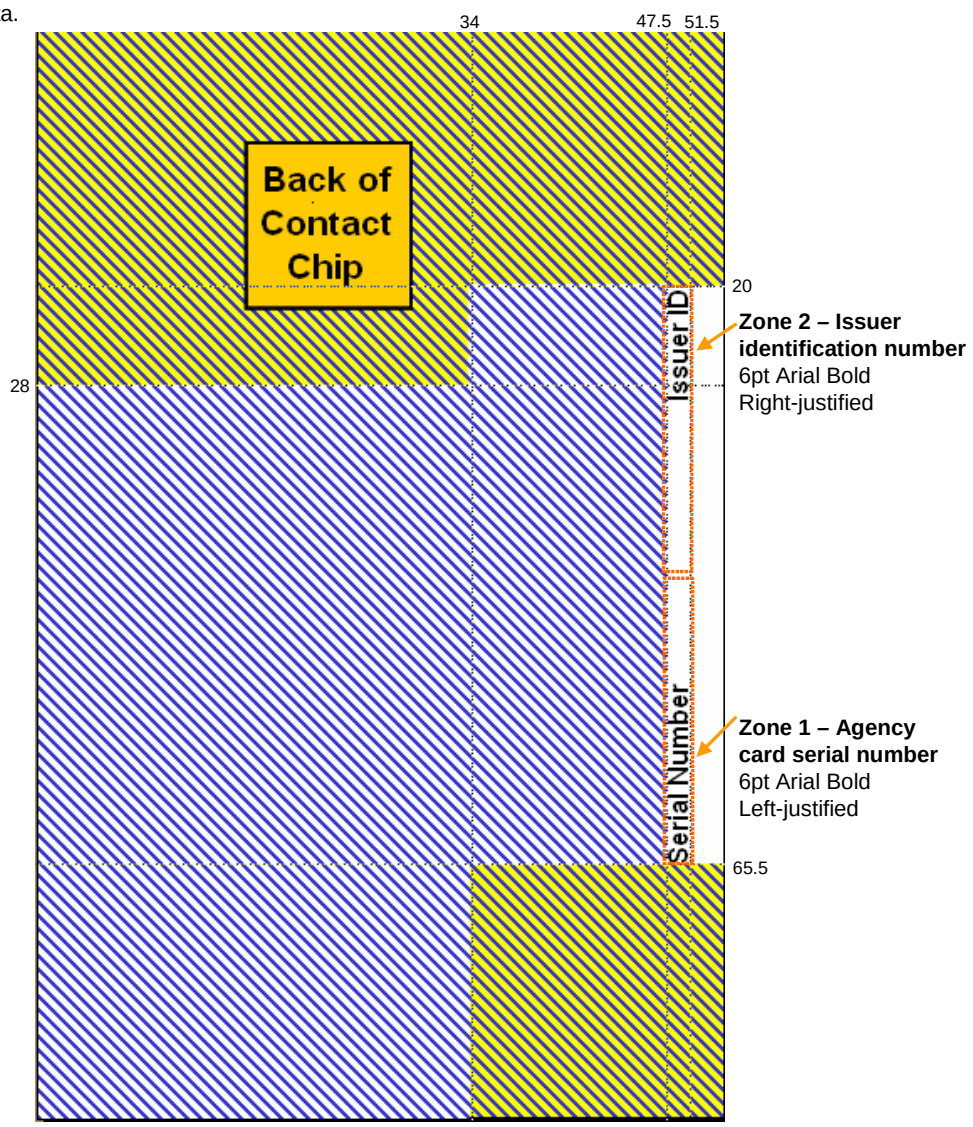


Figure 4-5. Card Front—Optional Data Placement—Example 4

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



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

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

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

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

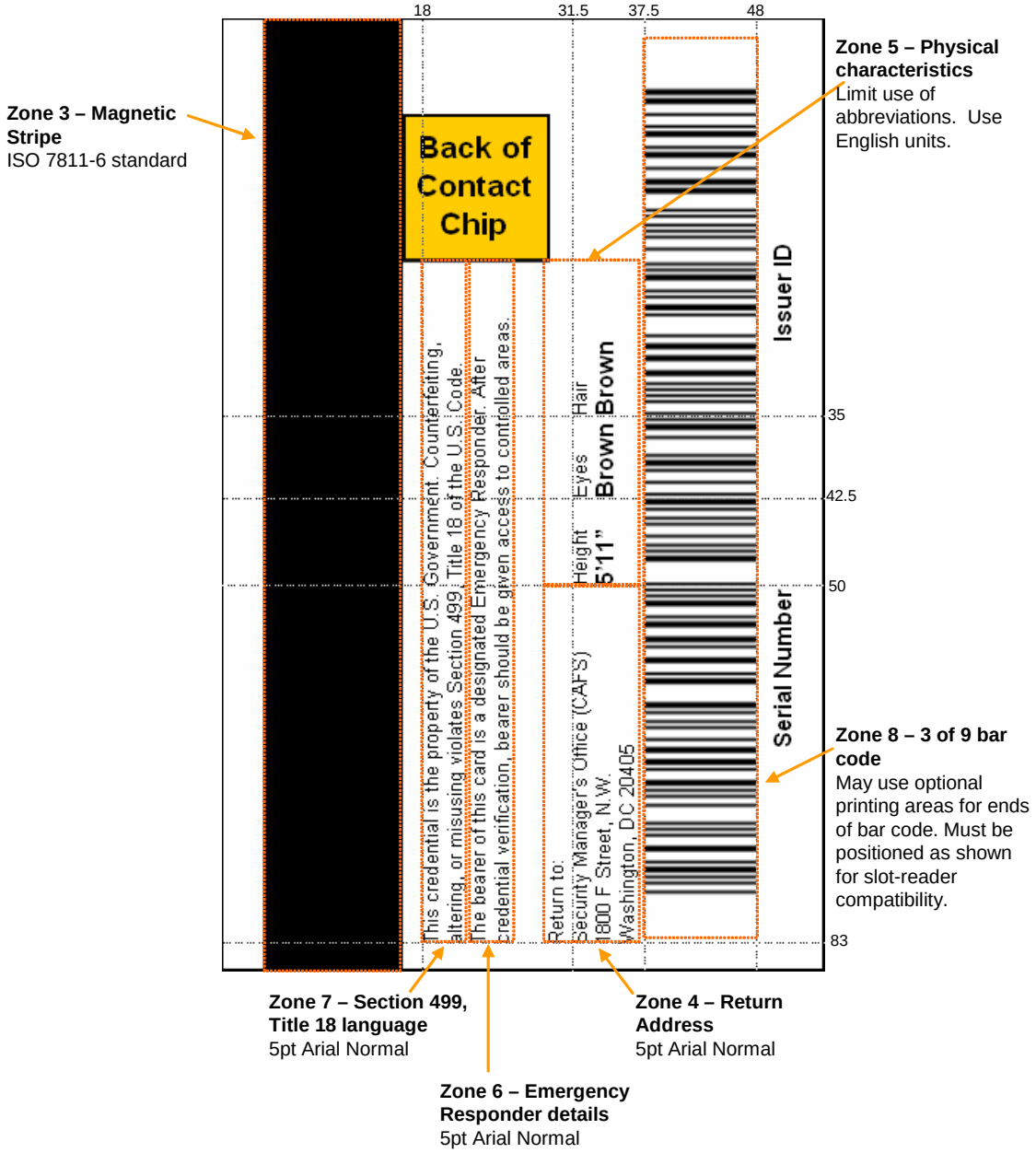
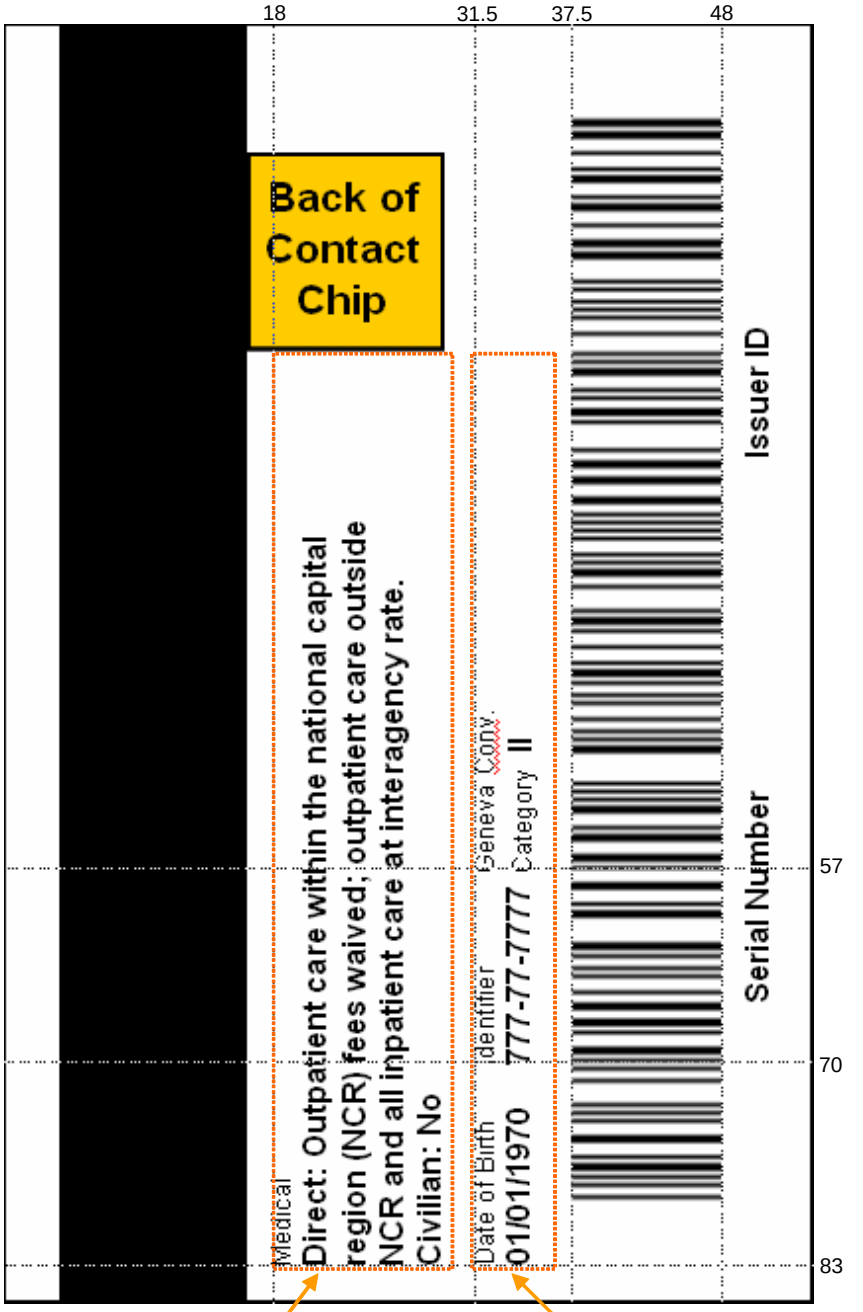


Figure 4-7. Card Back—Optional Data Placement—Example 1

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



Zone 9 – Agency specific text
Used instead of zones 6 & 7 (Medical example shown)

Zone 10 – Agency specific text
Used instead of zones 4 & 5 (DOB, ID, Geneva example shown)

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

4.1.5 Logical Credentials

This section defines logical identity credentials and the requirements for use of these credentials. Specifically, it provides details of the composition of an identity credential and its activation.

4.1.5.1 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 collectively comprise the data model for PIV logical credentials, and include the following:

+ A PIN
+ A CHUID
+ PIV authentication data (one asymmetric key pair and corresponding certificate)
+ Two biometric fingerprints.

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:

+ An asymmetric key pair and corresponding certificate for digital signatures
+ An asymmetric key pair and corresponding certificate for key management
+ Asymmetric or symmetric card authentication keys for supporting additional physical access applications
+ Symmetric key(s) associated with the card management system.

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.

PINs fall into the first category, card management keys into the second category, and the CHUID, biometric information, symmetric keys, and asymmetric keys into the third.

4.1.6 PIV Card Activation

The PIV Card must be activated[4] to perform privileged[5] operations such as reading biometric information and using asymmetric keys. The PIV Card shall be activated for privileged operations only after

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

authenticating the cardholder or the appropriate card management system. Cardholder authentication is described in Section 4.1.6.1, and card management system authentication is described in Section 4.1.6.2.

4.1.6.1 Activation by Cardholder

PIV Cards shall implement PIN-based cardholder activation to allow privileged operations using PIV credentials held by the card. For PIN-based cardholder activation, the cardholder shall supply a numeric PIN. The PIN shall be transmitted to the PIV Card and checked by the card. If the presented PIN is correct, the PIV Card is activated. The PIV Card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen. Moreover, the PIN should not be easily-guessable or otherwise individually-identifiable in nature (e.g., part of a Social Security Number, phone number). The PIN authentication mechanism shall meet the identity-based authentication requirements of FIPS PUB 140-2 Level 2. [FIPS140-2]

4.1.6.2 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 [SP800-73]. 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, Recommendation for Cryptographic Algorithms and Key Sizes. [SP800-78]

4.2 Cardholder Unique Identifier (CHUID)

The PACS Implementation Guidance [PACS] defines the CHUID data object; this description is refined in [SP800-73]. The PIV Card shall include the CHUID as defined in [SP800-73]. The CHUID includes an element, the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card. 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.

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. In machine readable format, the expiration date data element shall specify when the card expires. The expiration date format and encoding rules are as specified in [SP800-73]. For PIV Cards, the format of the asymmetric signature field is specified in Section 4.2.2.

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 3852 [RFC3852]. The digital signature shall be computed over the entire contents of the CHUID, excluding the Asymmetric Signature field. Algorithm and key size requirements for the asymmetric signature are detailed in [SP800-78].

The issuer asymmetric signature file is implemented as a *SignedData* Type, as specified in [RFC3852], and shall include the following information:

+ The message shall include a *version* field specifying version v3
+ The *digestAlgorithms* field shall be as specified in [SP800-78]
+ The *encapContentInfo* shall:
  - Specify an *eContentType* of id-PIV-CHUIDSecurityObject
  - Omit the *eContent* field
+ The *certificates* field shall include only a single X.509 certificate which can be used to verify the signature in the *SignerInfo* field
+ The *crls* field shall be omitted
+ *signerInfo*s shall be present and include only a single *SignerInfo*
+ The *SignerInfo* shall:
  - Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
  - Specify a *digestAlgorithm* in accordance with [SP800-78]
  - Include, at a minimum, the following signed attributes:
    - A *MessageDigest* attribute containing the hash computed over the concatenated contents of the CHUID, excluding the asymmetric signature field
    - 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 [COMMON], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3. The certificate shall also include an *extendedKeyUsage* extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix D.

4.3 Cryptographic Specifications

At a minimum, the PIV Card must store one asymmetric private key and a corresponding public key certificate, and perform cryptographic operations using the asymmetric private key. Cryptographic operations with this key are performed only through the contact interface.

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.

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. Cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a 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. 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.

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].

The PIV Card has a single mandatory key and four types of optional keys:

+ The *PIV authentication key* shall be an asymmetric private key supporting card authentication for an interoperable environment, and it is mandatory for each PIV Card.

+ The *card authentication key* may be either a symmetric (secret) key or an asymmetric private key 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.

+ The *card management key* is a symmetric key used for personalization and post-issuance activities, and it is optional.

All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule 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 of each class of keys 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).

  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. Section 5.4 of this document specifies the certificate format and the key management infrastructure for PIV authentication keys.

+ **Card Authentication Key.** The PIV Card shall not permit exportation of the card authentication key. Private/secret key operations may be performed using this key without explicit user action (e.g., the PIN need not be supplied). 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 5.4 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). This key is sometimes called an encryption key or an encipherment key.

  The PIV Card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5.4 of this document specifies the certificate format and the key management infrastructure for PIV key management keys.

+ **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. See Section 4.1.6.2 for further details.

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.

4.4 Biometric Data Specifications

The biometric data used during the PIV Card life cycle activities 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 facial image on the card as well as for performing visual authentication during card usage. A new facial image must be collected at the time of reissuance. The facial image is not required to be stored on the card.

+ Two electronic fingerprints to be stored on the card for automated authentication during card usage.

All three biometric data enumerated above are collected during the identity proofing and registration process. Implementation requirements for storage of biometric data on PIV Cards is dependent on use of specifications contained in NIST SP 800-76 [SP800-76].

The two electronic fingerprints stored on the card shall be accessible only over the contact interface and after the presentation of a valid PIN. No contactless access is permitted for the biometric data specified to be stored on the PIV Card under this standard.

4.4.1 Biometric Data Collection, Storage, and Usage

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]. 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.

A facial image shall be collected from all PIV applicants. The technical specifications for an electronic facial image are contained in [SP800-76]. The electronic facial image may be used for the following purposes:

- 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 cannot be collected from the PIV cardholder due to damage or injury to fingers
  - Fingerprint 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 [SP800-76]. 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 card fingerprints 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 fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography as described in Section 6.2.4.

4.4.2 Biometric Data Representation and Protection

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 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 CBEFF_SIGNATURE_BLOCK). [CBEFF] The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus facilitates the verification of integrity of the biometric data. 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]. 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 [RFC3852]. 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 STD_BIOMETRIC_RECORD). The algorithm and key requirements for the digital signature are the same as those 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 [SP800-78]
+ 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 as 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 [SP800-78]

  – Include at a minimum the following signed attributes:

    - A *MessageDigest* attribute containing the hash of the concatenated CBEFF_HEADER + STD_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 [COMMON], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3. The certificate shall also include an *extendedKeyUsage* extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix D.

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.

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 [SP800-76].

4.5 Card Reader Specifications

This section provides minimum requirements for the contact and contactless card readers. Also, this section provides requirements for PIN input devices.

4.5.1 Contact Reader Specifications

Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface. These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface in general desktop computing environment. 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 Specifications

Contactless card readers shall conform to the [ISO 14443] standard for the card-to-reader interface. 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. 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 PIN Input Device Specifications

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 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.

5.1 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.

5.2 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.

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 Inspector General as satisfying the requisite PIV objectives and requirements and approved in writing by the head of the Federal department or agency.

5.3 PIV Issuance and Maintenance Requirements

5.3.1 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 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. In such cases, the process must verify successful completion and adjudication of the investigation within six months of PIV card issuance, or the PIV card and the PIV authentication certificate for the card shall be revoked.

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.

5.3.2 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.

5.3.2.1 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.

5.3.2.2 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.

5.3.2.3 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.

5.3.2.4 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.

5.4 PIV Key Management Requirements

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

5.4.1 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 CRL Profile for the Common Policy* [PROF]. The requirements for legacy PKIs are defined in Section 5.4.4.

5.4.2 PKI Certificate

All certificates issued to support PIV Card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy[6] as defined in the *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework* [COMMON]. The requirements for legacy PKIs are defined in Section 5.4.4. These requirements cover identity proofing and the management of CAs and registration authorities. CAs and registration authorities may be operated by departments and agencies, or outsourced

[6] The id-CommonAuth policy has not yet been drafted. This policy will be used to differentiate simple authentication keys, where user interaction is not required, from signature keys where the operation is expected to demonstrate explicit user intent.

to PKI service providers. For a list of PKI service providers who have been approved to operate under [COMMON], see http://www.cio.gov/ficc/cpl.htm.

[COMMON] requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (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.

[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].

5.4.2.1 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:

+ 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.

+ Certificates containing the public key associated with an asymmetric Card Authentication Key must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension and must assert id-PIV-cardAuth in the extended key usage extension.

+ Certificates containing the public key associated with a digital signature private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF].

+ Certificates containing the public key associated with a PIV authentication private key shall conform to *Worksheet 5: End Entity Signature Certificate Profile* in [PROF], but shall not assert the nonRepudiation bit in the *keyUsage* extension and must include the PIV Card's FASC-N in the subject alternative name field.

+ Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].

+ Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP800-78].[7]

[7] The current text of [COMMON] permits only RSA with SHA-1 and SHA-256. Supporting the elliptic curve algorithms will require a change in [COMMON].

5.4.3 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].

5.4.4 Migration from Legacy PKIs

Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)

5.4.5 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 Certificate 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.

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

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

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

5.4.5.1 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 Table II—Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements of the Shared Service Provider Repository Service Requirements [SSP REP].

PIV Authentication certificates contain the FASC-N in the subject alternative name extension; hence, these certificates shall not be distributed publicly via LDAP or HTTP. Individual departments and agencies can decide whether other user certificates (digital signature and key management) can be distributed via LDAP. When user certificates are distributed, the requirements in Table I—End-Entity Certificate Repository Service Requirements of [SSP REP] shall be satisfied.

5.4.5.2 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].

5.5 PIV Privacy Requirements

The PIV Privacy Requirements stated in Section 2.4 apply equally to PIV-II implementations.

6. PIV Card Authentication

This section defines a suite of identity authentication mechanisms that are supported by the PIV Card, and their applicability in meeting the requirements for a set of graduated levels of identity assurance. 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, identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV Card. The authenticated identity can then be used to determine the permissions or authorizations that are granted to that identity to access various physical and logical resources.

6.1 Identity Authentication Assurance Levels

This standard defines three levels of assurance for identity authentication supported by the PIV Card. Each assurance level refers to the degree of confidence established in the identity of the holder of the PIV Card. The entity performing the authentication establishes confidence in the identity of the PIV cardholder through the following:

1) The rigor of the identity proofing process conducted prior to issuing the PIV Card

2) The security of the PIV Card issuance and maintenance processes.

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

Section 2 and 5 of this standard define requirements for the identity proofing, registration, issuance, and maintenance processes for all PIV Cards. Hence, there is a common level of assurance in these processes. The PIV Card bears a number of visual and logical credentials. Depending upon the specific PIV credentials 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:

+ 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 the discussion in Section 2 of OMB's E-Authentication Guidance for Federal Agencies, M-04-04 [OMB404]. Specifically, Table 6-1 shows the notional relationship between the PIV assurance levels and the [OMB404] 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 "identity assurance for electronic transactions requiring authentication" and prescribes a methodology 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 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 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 core (mandatory) credential set hosted by the PIV Card. 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.

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 parameters of the usage environment affect the PIV identity authentication mechanisms that may be applied to a particular situation.

Each authentication mechanism described in this section 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. The status of the PIV authentication certificate is directly tied to the status of all other credential elements held by the card.

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:

+ Photograph
+ Name
+ Employee affiliation employment identifier

+ Expiration date
+ Agency card serial number (back of card)
+ Issuer identification (back of card).

The PIV Card may also bear the following optional components:

+ Agency name and/or department
+ Department or agency seal
+ PIV cardholder's physical characteristics
+ Applicant's 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 employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Some of the 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
+ 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. (Optional)
3. The expiration date is checked to ensure that the card has not expired.
4. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Numbering System [DUNS]) are used as input to the authorization check to determine whether the cardholder should be granted access.

Some of the 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 hosts a mandatory signed biometric that can be read from the card following cardholder-to-card (CTC) authentication using a PIN supplied by the cardholder. The PIV biometric is 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 biometric.

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

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

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. (Optional)

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. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.

6.2.3.2 Attended Authentication of PIV Biometric (BIO-A)

The following sequence shall be followed for attended authentication of the PIV 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. (Optional)

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. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.

This authentication mechanism is similar to the unattended biometric credential check; 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.

6.2.4 Authentication Using PIV Asymmetric Cryptography (PKI)

The PIV Card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4. The following steps shall be used to perform authentication using the PIV asymmetric authentication key:

1. The cardholder is prompted to submit a PIN.

2. The submitted PIN is used to activate the card.

3. The reader issues a challenge string to the card and requests an asymmetric operation in response.

4. The card responds to the previously issued challenge by signing it using the PIV authentication private key and attaching the associated certificate.

5. 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.

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

7. The Subject Distinguished Name (DN) and FASC-N from the authentication certificate are extracted and passed as input to the authorization function.

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.

6.3 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 of the basic identity authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder.

6.3.1 Physical Access

The PIV Card can be used to authenticate 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. It is implicit that an authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

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
HIGH confidence	BIO
VERY HIGH confidence	BIO-A, PKI

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. It is implicit that an authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.

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
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, PKI	

Appendix A—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.

A.1 Role Based Model

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

A.1.1 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.

A.1.1.1 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.

A.1.1.2 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.

A.1.1.3 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.

A.1.2 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[8] 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[9] 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.

---

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

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

A.2 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.

A.2.1 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.

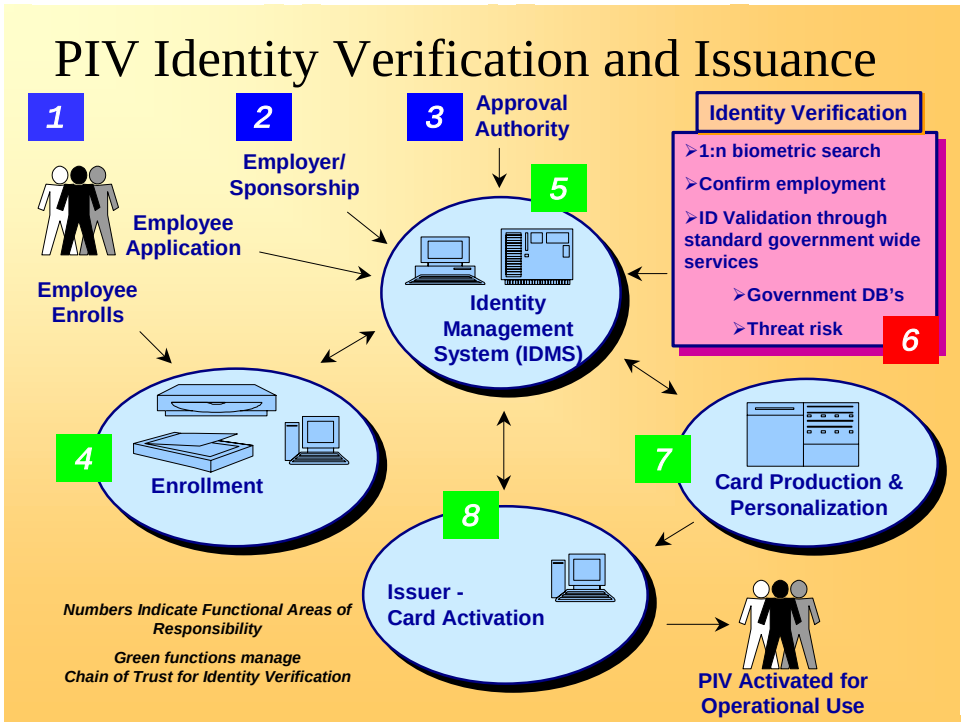


Figure A-1. PIV Identity Verification and Issuance

A.2.1.4 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.

A.2.1.5 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.

A.2.1.1.1 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.

A.2.1.1.2 PIV Application Process

The PIV Application Process has four components:

1. The Applicant request and claimed identity documentation,
2. The Employer/Sponsor approval of Applicant request,
3. The approval authority confirms and approves PIV application, appropriate sponsorship, and shall approve the PIV request,
4. 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.

A.2.1.1.3 PIV Enrollment Process

The PIV Enrollment process shall provide the following minimum steps:

1. Applicant shall appear for enrollment with supporting documentation;
2. Enrollment shall inspect and confirm all supporting documents using automated means if available;
3. Enrollment shall establish that the individual present matches the supporting documents;
4. Enrollment shall confirm Employer/Sponsor approval for PIV; and
5. Enrollment shall scan all supporting documents.

The PIV Binding process shall provide the following minimum steps:

1. Enrollment shall take biometric samples and photograph of the Applicant;
2. Enrollment shall manage the quality assurance process of the biometric and photographic capture. The biometric samples shall be verified to ensure proper performance; and
3. 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.

A.2.1.6 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:

1. Completed and signed PIV enrollment package;
2. Copies of the identity source documents;
3. Completed and signed background form received from the Applicant;
4. Results of the required background check;
5. Any other materials used to prove the identity of the Applicant;
6. The credential identifier such as an identity credential serial number;
7. The expiration date of the identity credential;
8. Unique minimal identity record for each approved Applicant;
9. Separated database indexed to the minimal identity record containing the original biometric data captured at enrollment. These data shall be encrypted at rest; and
10. Separated database of biometric data indexed to the minimal identity record supporting AFIS for 1:many identity checking.

The IDMS shall provide services that:

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

2. Notify the Employer of status of the PIV; and
3. 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.

A.2.2 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—

1. Maintain full inventory control of blank initialized or pre-issued (e.g. with the manufacturers keys) stock, consumables and manufacturing materials;
2. Maintain a list of approved IDMS systems that can submit PIV requests for card production,
3. Provide acknowledgement of IDMS request to produce a PIV;
4. Notify the IDMS upon completion of PIV credential production;
5. Maintain a list of approved Issuers that can activate and issue PIV credentials;
6. Only send information regarding production of PIV credentials to approved authorities;
7. Only send fully completed and personalized PIV credentials to approved Issuing Agents; and
8. 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.

A.2.3 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.

A.2.4 Re-issuance to Current PIV Credential Holders

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

1. Insure the IDMS record for this individual states the credential is not expired;
2. Verify the individual with a 1:1 biometric match against the IDMS record;
3. Verify the individual against the IDMS record digital photograph;
4. Recapture biometrics;

5. Issue a new credential and update the IDMS record; and
6. The recaptured biometrics and new credential record shall be digitally signed by the Issuing Authority.

Appendix B—PIV Validation, Certification, and Accreditation

B.1 Accreditation of PIV Service Providers

[HSPD-12] requires that all cards be issued by providers whose reliability has been established by an official accreditation process. Funding permitting, NIST will establish detailed criteria that PIV Card issues must meet for accreditation. Additionally, NIST will (again, funding permitting) establish a government-wide program to accredit official issuers of PIV Cards against these accreditation criteria. Until such time as these are completed, agencies must self-certify their own issuers of PIV Cards.

B.2 Security Certification and Accreditation of IT System(s)

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]

B.3 Conformance of PIV Components to this Standard

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 http://csrc.nist.gov/PIV-Project/Conformance/ 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

B.4 Cryptographic Testing and Validation (FIPS 140-2 and algorithm standards)

All the cryptographic modules in the PIV system (both on-card and issuer software) shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher). [FIPS140-2] The facilities for FIPS 140-2 testing are the Cryptographic Module Testing (CMT) laboratories accredited by the National Voluntary Laboratory Accreditation Program (NVLAP) program of NIST. Vendors wanting to supply

cryptographic modules for the PIV system can select any of the accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor module is issued by the Cryptographic Module Validation Program (CMVP), 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.ncsl.nist.gov/cryptval.

Appendix C—Background Check Descriptions

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

+ **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.

+ **NACI.** The basic and minimum investigation required on all new Federal employees consisting of a 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:

  – Employment, 5 years

  – Education, 5 years and highest degree verified

  – Residence, 3 years

  – References

  – Law Enforcement, 5 years

  – NACs

Appendix D—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	2.16.840.1.101.3.7.1.1.4.3.1	The associated content is the concatenated contents of the CHUID, excluding the authentication key map and the asymmetric signature field.
id-PIV-biometricObject	2.16.840.1.101.3.7.1.1.4.2.1	The associated content is the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD.
id-PIV-authCertificateObject	2.16.840.1.101.3.7.1.1.2.2.1	The associated content is the public key certificate associated with the PIV authentication key.
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 attribute value is of type OCTET STRING and 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.

Appendix E—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

Appendix F—Glossary of Terms, Acronyms, and Notations

F.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).

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 iriscan 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:

+ 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 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.

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.

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

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.

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 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.

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

Key: See "Cryptographic Key".

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

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

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.

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]

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

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.

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".

F.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
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Cardholder Unique Identifier
CIA	Cryptographic Information Application
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
DCII	Defense Clearance and Investigation Index
DN	Distinguished Name

dpi	Dots Per Inch
DUNS	Data Universal Numbering System
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ERT	Emergency Response Team
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certificate 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
HMAC	Hash-Based Message Authentication Code
HR	House of Representatives
HSPD	Homeland Security Presidential Directive
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
JPEG	Joint Photographic Experts Group
LDAP	Lightweight Directory Access Protocol
MAC	Message Authentication Code
MQV	Menezes-Qu-Vanstone
NAC	National Agency Check
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
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

PACS	Physical Access Control System
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
pt	Point
RFC	Request for Comment
RSA	Rivest Shamir Adleman
SF	Standard Form
SHA	Secure Hash Algorithm
SII	Security/Suitability Investigations Index
SP	Special Publication
SSP REP	Shared Service Provider Repository Service Requirement
URI	Uniform Resource Identifier

F.3 Notations

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, this standard uses the following typographical conventions in text:

+ Terms (word or concatenated words) in *Italics* represent ASN.1 data types. For example, *SignedData or 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.

Appendix G—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 2.0, November 1, 2004. Available at http://www.cio.gov/ficc/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.

[FIPS140-2] FIPS Publication 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001. 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.

[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.

[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.

[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 CRL Profile for the Common Policy*, Version 1.1, July 8, 2004. Available at http://www.cio.gov/ficc/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.

[RFC3280] RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*, IETF, April 2002. Available at http://www.ietf.org/rfc/rfc3280.txt.

[RFC3852] RFC 3852, *Cryptographic Message Syntax (CMS)*, IETF, July 2004. Available at http://www.ietf.org/rfc/rfc3852.txt.

[SP800-37] NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST, May 2004.

[SP800-53] NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, NIST, September 2004 (2PD).

[SP800-63] NIST Special Publication 800-63, *Electronic Authentication Guideline*, Appendix A, NIST, June 2004.

[SP800-73] NIST Special Publication 800-73, *Integrated Circuit Card for Personal Identity Verification*, NIST, February 2005.

[SP800-76] NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, NIST, February 2005.

[SP800-78] NIST Special Publication 800-78, *Recommendation for Cryptographic Algorithms and Key Sizes*, NIST, February 2005.

[SSP REP] Shared Service Provider Repository Service Requirements, January 23, 2004. Available at http://www.cio.gov/ficc/documents/SSPrepositoryRqmts.pdf.