FIPS PUB 201-2

FEDERAL INFORMATION PROCESSING STANDARDS PUBLICATION

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

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

July 2012

U.S. DEPARTMENT OF COMMERCE
Rebecca M. Blank, Acting Secretary

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

Acknowledgements

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

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

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.

Charles H. Romine, 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 the minimum requirements for a Federal personal identity verification system that meets the control and security objectives of Homeland Security Presidential Directive-12 [HSPD-12], including identity proofing, registration, and issuance. The Standard also provides detailed specifications that will support technical interoperability among PIV systems of Federal departments and agencies. It describes the card elements, system interfaces, and security controls required to securely store, process, and retrieve identity credentials from the card. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this Standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in Special Publication 800-73, *Interfaces for Personal Identity Verification*. The interfaces and data formats of biometric information are specified in Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*. The requirements for cryptographic algorithms are specified in Special Publication 800-78, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the accreditation of the PIV Card issuers are specified in Special Publication 800-79, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*. The unique organizational codes for Federal agencies are assigned in Special Publication 800-87, *Codes for the Identification of Federal and Federally-Assisted Organizations*. The requirements for card readers are specified in Special Publication 800-96, *PIV Card to Reader Interoperability Guidelines*. The format for encoding the chain-of-trust for import and export is specified in Special Publication 800-156, *Representation of PIV Chain-of-Trust for Import and Export*. The requirements for issuing PIV derived credentials are specified in Special Publication 800-157, *Guidelines for Personal Identity Verification (PIV) Derived Credentials*.

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, public key infrastructure, PKI, validation, verification.

Federal Information Processing Standards 201
2012

Announcing the
Standard for

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

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

1. Name of Standard.

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

2. Category of Standard.

Information Security.

3. Explanation.

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

(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 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. 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.

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

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 threats from outside the contiguous United States, the issuance, holding, and/or use of PIV Cards 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 Cards, 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 interagency interoperability and the President's policy. Use of other risk-mitigating technical (e.g., high-assurance on-off switches for the wireless capability) and procedural mechanisms in such situations is preferable, and as such is also explicitly permitted and encouraged. As protective security technology advances, the need for this provision will be re-assessed as the Standard undergoes the normal review and update process.

7. Specifications.

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

8. Implementations.

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

A PIV Card must be personalized with identity information for the individual to whom the card is issued, in order to perform identity verification both by humans and automated systems. Humans can use the physical card for visual comparisons, whereas automated systems can use the electronically stored data on the card to conduct automated identity verification. In implementing PIV systems and pursuant to Section 508 of the Rehabilitation Act of 1973 (the Act), as amended, agencies have the responsibility to accommodate federal employees and contractors with disabilities to have access to and use of information and data comparable to the access to and use of such information and data by federal employees and contractors who are not individuals with disabilities. In instances where Federal agencies assert exceptions to Section 508 accessibility requirements (e.g., undue burden, national security, commercial non-availability), Sections 501 and 504 of the Act requires Federal agencies to provide reasonable accommodation for federal employees and contractors with disabilities whose needs are not met by the baseline accessibility provided under Section 508. While Section 508 compliance is the responsibility of

Federal agencies and departments, this Standard specifies options to aid in implementation of the requirements:

- Section 4.1.4.3 specifies Zones 21F and 22F as an option for orientation markers of the PIV Card.
- Section 2.8 describes an alternative to the National Criminal History Check (NCHC) in instances where an applicant has unclassifiable fingers.
- Sections 2.8, and 2.9 specify alternative methods for the 1:1 biometric match required at PIV Card issuance, reissuance, renewal, and reset.
- Section 6 defines authentication mechanisms with varying characteristics for both physical and logical access (e.g., with or without PIN, over contact, contactless, or virtual contact interface).

Federal departments and agencies must use accredited issuers to issue identity credentials for Federal employees and contractors. For this purpose, NIST provided guidelines for the accreditation of PIV Card issuers in [SP 800-79]. The Standard also covers security and interoperability requirements for PIV Cards. For this purpose, NIST has established the PIV Validation Program that tests implementations for conformance with this Standard as specified in [SP 800-73] and [SP 800-78]. Additional information on this program is published and maintained at http://csrc.nist.gov/groups/SNS/piv/npivp/. The U.S. General Services Administration (GSA) has set up the FIPS 201 Evaluation Program to evaluate conformance of different families of products that support the PIV processes of this Standard – see Appendix A.5.

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

9. Effective Date.

This Standard is effective immediately and supersedes FIPS 201-1 (Change Notice 1). New optional features of this Standard that depend upon the release of new or revised NIST Special Publications are effective upon final publication of the supporting Special Publications.

10. Implementation Schedule.

This Standard mandates the implementation of some of the PIV Card features that were optional to implement in FIPS 201-1. To comply with FIPS 201-2, all new and replacement PIV Cards shall be issued with the mandatory PIV Card features no later than 12 months after the effective date of this Standard.

Accreditations of PIV Card issuers (PCIs) that occur 12 months after the effective date of this Standard shall be in compliance with FIPS 201-2.

FIPS 201-2 compliance of PIV components and subsystems is provided in accordance with M-06-18 [OMB0618] and M-11-11 [OMB1111] through products and services from GSA's Interoperability Test Program and Approved Products and Services List, once available. Implementation Guidance to PIV enabled federal facilities and information systems, in accordance to M-11-11 will be outlined in the "Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance."

11. 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; and
- protection provided to the identity verification system infrastructure and components throughout the entire lifecycle.

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, NIST has a policy to review this Standard within five years to assess its adequacy.

12. Waivers.

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

13. Where to Obtain Copies.

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

14. Patents.

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

Table of Contents

1. Introduction 1

1.1 Purpose 1
1.2 Scope 1
1.3 Change Management 2
1.3.1 Backward Compatible Change 2
1.3.2 Non-Backward Compatible Change 2
1.3.3 New Features 2
1.3.4 Deprecated and Removed 2
1.3.5 FIPS 201 Version Management 3
1.4 Document Organization 3

2. Common Identification, Security, and Privacy Requirements 5

2.1 Control Objectives 5
2.2 Credentialing Requirements 6
2.3 Biometric Data Collection for Background Investigations 6
2.4 Biometric Data Collection for PIV Card 6
2.5 Biometric Data Use 7
2.6 Chain-of-Trust 7
2.7 PIV Identity Proofing and Registration Requirements 8
2.8 PIV Card Issuance Requirements 10
2.8.1 Special Rule for Pseudonyms 11
2.8.2 Grace Period 12
2.9 PIV Card Maintenance Requirements 12
2.9.1 PIV Card Renewal Requirements 12
2.9.2 PIV Card Reissuance Requirements 13
2.9.3 PIV Card Post Issuance Update Requirements 14
2.9.4 PIV Card Verification Data Reset 15
2.9.5 PIV Card Termination Requirements 16
2.10 PIV Derived Credentials Issuance Requirements 16
2.11 PIV Privacy Requirements 17

3. PIV System Overview 19

3.1 Functional Components 19
3.1.1 PIV Front-End Subsystem 20
3.1.2 PIV Card Issuance and Management Subsystem 21
3.1.3 PIV Relying Subsystem 21
3.2 PIV Card Lifecycle Activities 22

4. PIV Front-End Subsystem 24

4.1 PIV Card Physical Characteristics 24
4.1.1 Printed Material 24
4.1.2 Tamper Proofing and Resistance 24
4.1.3 Physical Characteristics and Durability 25
4.1.4 Visual Card Topography 26
4.1.5 Color Representation 40
4.2 PIV Card Logical Characteristics 40
4.2.1 Cardholder Unique Identifier (CHUID) 41
4.2.2 Cryptographic Specifications 42

4.2.3 PIV Biometric Data Specifications 44
4.2.4 PIV Unique Identifiers 46
4.3 PIV Card Activation 46
4.3.1 Activation by Cardholder 46
4.3.2 Activation by Card Management System 47
4.4 Card Reader Requirements 47
4.4.1 Contact Reader Requirements 47
4.4.2 Contactless Reader Requirements 47
4.4.3 Reader Resilience and Flexibility 47
4.4.4 Card Activation Device Requirements 48

5. PIV Key Management Requirements 49

5.1 Architecture 49
5.2 PKI Certificate 49
5.2.1 X.509 Certificate Contents 49
5.3 X.509 CRL Contents 50
5.4 Legacy PKIs 50
5.5 PKI Repository and OCSP Responder(s) 50
5.5.1 Certificate and CRL Distribution 50
5.5.2 OCSP Status Responders 51

6. PIV Cardholder Authentication 52

6.1 PIV Assurance Levels 52
6.1.1 Relationship to OMB's E-Authentication Guidance 53
6.2 PIV Card Authentication Mechanisms 53
6.2.1 Authentication Using Off-Card Biometric Comparison 53
6.2.2 Authentication Using On-Card Biometric Comparison (OCC-AUTH) 55
6.2.3 Authentication Using PIV Asymmetric Cryptography 55
6.2.4 Authentication with the Symmetric Card Authentication Key (SYM-CAK) 57
6.2.5 Authentication Using the CHUID 57
6.2.6 Authentication Using PIV Visual Credentials (VIS) 58
6.3 PIV Support of Graduated Assurance Levels for Identity Authentication 59
6.3.1 Physical Access 59
6.3.2 Logical Access 60

List of Appendices

Appendix A— PIV Validation, Certification, and Accreditation 61

A.1 Accreditation of PIV Card Issuers (PCI) 61
A.2 Application of Risk Management Framework to IT System(s) Supporting PCI 62
A.3 Conformance Testing of PIV Card Application and Middleware 62
A.4 Cryptographic Testing and Validation 62
A.5 FIPS 201 Evaluation Program 62

Appendix B— PIV Object Identifiers and Certificate Extension 63

B.1 PIV Object Identifiers 63
B.2 PIV Certificate Extension 63

Appendix C— Glossary of Terms, Acronyms, and Notations 65

C.1 Glossary of Terms 65
C.2 Acronyms 69
C.3 Notations 71

Appendix D— References 72

Appendix E— Revision History 76

List of Figures

Figure 3-1. PIV System Notional Model 20
Figure 3-2. PIV Card Lifecycle Activities 22
Figure 4-1. Card Front—Printable Areas and Required Data 32
Figure 4-2. Card Front—Optional Data Placement—Example 1 33
Figure 4-3. Card Front—Optional Data Placement—Example 2 34
Figure 4-4. Card Front—Optional Data Placement—Example 3 35
Figure 4-5. Card Front—Optional Data Placement—Example 4 36
Figure 4-6. Card Back—Printable Areas and Required Data 37
Figure 4-7. Card Back—Optional Data Placement—Example 1 38
Figure 4-8. Card Back—Optional Data Placement—Example 2 39

List of Tables

Table 4-1. Name Examples 27
Table 4-2. Color Representation 40
Table 6-1. Relationship Between PIV and E-Authentication Assurance Levels 53
Table 6-2. Authentication for Physical Access 60
Table 6-3. Authentication for Logical Access 60
Table B-1. PIV Object Identifiers 63

1. Introduction

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

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

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

1.1 Purpose

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

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

1.2 Scope

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

(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.

This Standard defines authentication mechanisms offering varying degrees of security for both logical and physical access applications. Federal departments and agencies will determine the level of security and authentication mechanisms appropriate for their applications. This Standard does not specify access control policies or requirements for Federal departments and agencies. Therefore, the scope of this Standard is limited to authentication of an individual's identity. Authorization and access control decisions are outside the scope of this Standard. Moreover, requirements for a temporary card used until a new or replacement PIV Card arrives are out of scope of this Standard.

1.3 Change Management

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

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

1.3.1 Backward Compatible Change

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

1.3.2 Non-Backward Compatible Change

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

1.3.3 New Features

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

1.3.4 Deprecated and Removed

When a feature is discontinued or no longer needed, it is deprecated. Such a feature remains in the current Standard as an optional feature but its use is strongly discouraged. A deprecated feature does not affect existing systems but should be phased out in future systems, because the feature will be removed in the next revision of the Standard. For example, existing PIV Cards with deprecated data elements remain

valid until they naturally expire. Replacement PIV Cards, however, should not re-use the deprecated features because the next revision of the Standard will remove the support for deprecated data elements.

1.3.5 FIPS 201 Version Management

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

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

1.4 Document Organization

This Standard describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of [HSPD-12], including identity proofing, registration, and issuance. It provides detailed technical specifications to support the control and security objectives of [HSPD-12] as well as interoperability among Federal departments and agencies. This Standard describes the policies and minimum requirements of a PIV Card that allows interoperability of credentials for physical and logical access. The physical card characteristics, storage media, and data elements that make up identity credentials are specified in this Standard. The interfaces and card architecture for storing and retrieving identity credentials from a smart card are specified in 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 Special Publication 800-76 [SP 800-76], *Biometric Data Specification for Personal Identity Verification*. The requirements for cryptographic algorithms are specified in Special Publication 800-78 [SP 800-78], *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*. The requirements for the accreditation of PIV Card issuers are specified in Special Publication 800-79 [SP 800-79], *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*. The unique organizational codes for Federal agencies are assigned in Special Publication 800-87 [SP 800-87], *Codes for the Identification of Federal and Federally-Assisted Organizations*. The requirements for the PIV Card reader are provided in Special Publication 800-96 [SP 800-96], *PIV Card to Reader Interoperability Guidelines*. The format for encoding the chain-of-trust for import and export is specified in Special Publication 800-156 [SP 800-156], *Representation of PIV Chain-of-Trust for Import and Export*. The requirements for issuing PIV derived credentials are specified in Special Publication 800-157 [SP 800-157], *Guidelines for Personal Identity Verification (PIV) Derived Credentials*.

This Standard contains normative references to other documents, and to the extent described in each citation these documents are included by reference in this Standard. Should normative text in this Standard conflict with normative text in a referenced document the normative text in this Standard prevails for this Standard.

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

- Section 1, Introduction, provides background information for understanding the scope of this Standard. This section is *informative*.

- Section 2, Common Identification, Security, and Privacy Requirements, outlines the requirements for identity proofing, registration, and issuance, by establishing the control and security objectives for compliance with [HSPD-12]. This section is *normative.*

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

- Section 4, PIV Front-End Subsystem, provides the requirements for the components of the PIV front-end subsystem. Specifically, this section defines requirements for the PIV Card, logical data elements, biometrics, cryptography, and card readers. This section is *normative*.

- Section 5, PIV Key Management Requirements, defines the processes and components required for managing a PIV Card's lifecycle. It also provides the requirements and specifications related to this subsystem. This section is *normative*.

- Section 6, PIV Cardholder Authentication, defines a suite of authentication mechanisms that are supported by the PIV Card, and their applicability in meeting the requirements of graduated levels of identity assurance. This section is *normative.*

- Appendix A, PIV Validation, Certification, and Accreditation, provides additional information regarding compliance with this document. This appendix is *normative*.

- Appendix B, PIV Object Identifiers and Certificate Extension, provides additional details for the PIV objects identified in Section 4. This appendix is *normative*.

- Appendix C, Glossary of Terms, Acronyms, and Notations, describes the vocabulary and textual representations used in the document. This appendix is *informative*.

- Appendix D, References, lists the specifications and standards referred to in this document. This appendix is *informative.*

- Appendix E, Revision History, lists changes made to this Standard from its inception. This appendix is *informative.*

2. Common Identification, Security, and Privacy Requirements

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

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

2.2 Credentialing Requirements

Federal departments and agencies shall use the credentialing guidance issued by the Director of the Office of Personnel Management (OPM) to heads of departments and agencies when determining whether to issue or revoke PIV Cards (e.g., [SPRINGER MEMO], [FIS][2]). In addition to OPM's [FIS], Federal department and agencies shall also apply credentialing requirements specified in applicable OMB memoranda (e.g., OMB Memorandum M-05-24 [OMB0524]).

2.3 Biometric Data Collection for Background Investigations

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

+ A full set of fingerprints. Biometric identification using fingerprints is the primary input to law enforcement checks. In cases where ten fingerprints are not available, then as many fingers as possible shall be imaged. In cases where obtaining any fingerprints is impossible, agencies shall seek OPM guidance for alternative means of performing the law enforcement checks.

This collection is not necessary for applicants who have a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation that can be located and referenced.

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

2.4 Biometric Data Collection for PIV Card

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

+ Two fingerprints, for off-card comparison. These shall be taken either from the full set of fingerprints collected in Section 2.3, or collected independently.

+ An electronic facial image.

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

+ One or two iris images.

+ Two fingerprints, for on-card comparison, which may be the same as the two fingerprints collected for off-card comparison.

If the biometric data that is collected as specified in this section and in Section 2.3 is collected on separate occasions, then a 1:1 biometric match of the applicant shall be performed at each visit against biometric data collected during a previous visit.

Biometric data collection shall be conformant to the procedural and technical specifications of [SP 800-76]. The choice of which two fingers is important and may vary between persons. The recommended selection and order is specified in [SP 800-76].

[2] Federal Investigative Standards. [URL will be added for OPM's new investigative standard once published ~July 2012.]

2.5 Biometric Data Use

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

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

The optional fingerprints may be used for preparation of the fingerprint templates for on-card comparison as described in Section 4.2.3.1. OCC may be used to support card activation as described in Section 4.3.1 and cardholder authentication as described in Section 6.2.2.

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

The electronic facial image:

+ shall be stored on the PIV Card as described in Section 4.2.3.1;

+ shall be printed on the PIV Card according to Section 4.1.4.1;

+ may be used for generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.6; and

+ may be used for biometric authentication in operator-attended PIV issuance, reissuance, renewal and verification data reset processes.

2.6 Chain-of-Trust

A card issuer may optionally maintain, for each PIV Card issued, a documentary chain-of-trust for the identification data it collects. The chain-of-trust is a sequence of related enrollment data records that are created and maintained through the methods of contemporaneous acquisition of data within each enrollment data record, and biometric matching of samples between enrollment data records.[3]

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

+ A log of activities that documents who took the action, what action was taken, when and where the action took place, and what identification data was collected.

+ An enrollment data record that contains the most recent collection of each of the biometric data collected. The enrollment data record describes the circumstances of biometric acquisition including the name and role of the acquiring agent, the office and organization, time, place, and acquisition

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

method. The enrollment data record may also document unavailable biometric data or failed attempts to collect biometric data. The enrollment data record may contain historical biometric data.

- The most recent unique identifiers (i.e., Federal Agency Smart Credential Number (FASC-N) and Universally Unique IDentifier (UUID)) issued to the individual. The record may contain historical unique identifiers.
- Information about the authorizing entity who has approved the issuance of a credential.
- Current status of the background investigation, including the results of the investigation once completed.
- The evidence of authorization if the credential is issued under a pseudonym.
- Any data or any subsequent changes in the data about the cardholder. If the changed data is the cardholder's name, then the issuer should include the evidence of a formal name change.

The biometric data in the chain-of-trust shall be valid for at most 12 years. In order to mitigate ageing effects and thereby maintain operational readiness of a cardholder's PIV Card, agencies may require biometric enrollment more frequently than 12 years.

The chain-of-trust contains personally identifiable information (PII). If implemented, it shall be protected in a manner that protects the individual's privacy and maintains the integrity of the chain-of-trust record both in transit and at rest. A card issuer may import and export a chain-of-trust in the manner and representation described in [SP 800-156].

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

- Extended enrollment: a PIV applicant enrolls a full set of fingerprints for background investigations at one place and time, and two fingerprints for the PIV Card at another place and time. The chain-of-trust would contain identifiers and two enrollment data records, one with a full-set fingerprint transaction, and one with two fingerprint templates. The two fingerprint templates would be matched against the corresponding fingers in the ten-fingerprint data set to link the chain.
- Reissuance: a PIV cardholder loses his/her card. Since the card issuer has biometric enrollment data records, the cardholder can perform a 1:1 biometric match to reconnect to the card issuer's chain-of-trust. The card issuer need not repeat the identity proofing and registration process. The card issuer proceeds to issue a new card as described in Section 2.9.2.
- Interagency transfer: a Federal employee is transferred from one agency to another. When the employee leaves the old agency, he/she surrenders the PIV Card and it is destroyed. When the employee arrives at the new agency and is processed in, the card issuer in the new agency requests the employee's chain-of-trust from the card issuer in the old agency, and receives the chain-of-trust. The employee performs a 1:1 biometric match against the chain-of-trust, and the interaction proceeds as described in Section 2.8.2.

2.7 PIV Identity Proofing and Registration Requirements

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

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

+ Biometrics shall be captured as specified in Sections 2.3 and 2.4.

+ The process shall begin by locating and referencing a completed and favorably adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation record. In the absence of a record, the process shall ensure 1) the initiation of a Tier 1 or higher federal background investigation and 2) the completion of the Automated Record Checks (ARC) of the background investigation. In cases where the ARC results are not received within 5 days of the ARC initiation, the FBI NCHC (fingerprint check) portion of the ARC shall be complete before credential issuance.

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

+ During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form.[4] The identity source documents shall be bound to that applicant and shall be neither expired nor cancelled. If the two identity source documents bear different names, evidence of a formal name change shall be provided. The primary identity source document shall be one of the following forms of identification:

  - a U.S. Passport or a U.S. Passport Card;
  - a Permanent Resident Card or an Alien Registration Receipt Card (Form I-551);
  - a foreign passport;
  - an Employment Authorization Document that contains a photograph (Form I-766);
  - a Driver's license or an ID card issued by a state or possession of the United States provided it contains a photograph;
  - a U.S. Military ID card;
  - a U.S. Military dependent's ID card; or
  - a PIV Card.

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

  - a U.S. Social Security Card issued by the Social Security Administration;
  - an original or certified copy of a birth certificate issued by a state, county, municipal authority, possession, or outlying possession of the United States bearing an official seal;
  - an ID card issued by a federal, state, or local government agency or entity, provided it contains a photograph;

[4] Departments and agencies may choose to accept only a subset of the identity source documents listed in this section. For example, in cases where identity proofing for PIV Card issuance is performed prior to verification of employment authorization, departments and agencies may choose to require the applicant to provide identity source documents that satisfy the requirements of Form I-9, *Employment Eligibility Verification*, in addition to the requirements specified in this section.

- a voter's registration card;
- a U.S. Coast Guard Merchant Mariner Card;
- a Certificate of U.S. Citizenship (Form N-560 or N-561);
- a Certificate of Naturalization (Form N-550 or N-570);
- a U.S. Citizen ID Card (Form I-197);
- an Identification Card for Use of Resident Citizen in the United States (Form I-179);
- a Certification of Birth Abroad or Certification of Report of Birth issued by the Department of State (Form FS-545 or Form DS-1350);
- a Temporary Resident Card (Form I-688);
- an Employment Authorization Card (Form I-688A);
- a Reentry Permit (Form I-327);
- a Refugee Travel Document (Form I-571);
- an Employment authorization document issued by Department of Homeland Security (DHS);
- an Employment Authorization Document issued by DHS with photograph (Form I-688B);
- a driver's license issued by a Canadian government entity; or
- a Native American tribal document.

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

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

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

2.8 PIV Card Issuance Requirements

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

+ Credentials are issued after a proper authority has authorized issuance of the credential.

544 + The organization shall use an approved PIV credential issuance process in accordance with
545 [SP 800-79].

546 + Before issuing the identity credential, the process shall ensure that a previously completed and favorably
547 adjudicated NACI (or equivalent or higher) or Tier 1 or higher federal background investigation is on
548 record. In the absence of a record, the required federal background investigation shall be initiated. The
549 credential should not be issued before the results of the ARC are complete. However, if the results of the
550 ARC have not been received in 5 days, the identity credential may be issued based on the FBI NCHC. In
551 the absence of an FBI NCHC (e.g., due to unclassifiable fingerprints) the ARC results are required prior to
552 issuing a PIV Card. The PIV Card shall be revoked if the results of the background investigation so justify.

553 + Biometrics used to personalize the PIV Card must be those captured during the identity proofing and
554 registration process.

555 + During the issuance process, the issuer shall verify that the individual to whom the credential is to be
556 issued is the same as the intended applicant/recipient as approved by the appropriate authority.
557 Before the card is provided to the applicant, the issuer shall perform a 1:1 biometric match of the
558 applicant against biometrics available on the PIV Card. The 1:1 biometric match requires either a
559 match of fingerprint(s) or, if unavailable, other optional biometric data that are available. Minimum
560 accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the
561 PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is
562 available, the cardholder shall provide two identity source documents (as specified in Section 2.7),
563 and an attending operator shall inspect these and compare the cardholder with the facial image printed
564 on the PIV Card.

565 + The organization shall issue PIV credentials only through systems and providers whose reliability has
566 been established by the agency and so documented and approved in writing (i.e., accredited) in
567 accordance with [SP 800-79].

568 + The PIV Card shall be valid for no more than six years.

569 PIV Cards that contain topographical defects (e.g., scratches, poor color, fading, etc.) or that are not
570 properly printed shall be destroyed. The PIV Card issuer is responsible for the card stock, its
571 management, and its integrity.

572 ### 2.8.1 Special Rule for Pseudonyms

573 In limited circumstances Federal employees and contractors are permitted to use pseudonyms during the
574 performance of their official duties with the approval of their employing agency. If an agency determines
575 that use of a pseudonym is necessary to protect an employee or contractor (e.g., from physical harm,
576 severe distress, or harassment),[5] the agency may formally authorize the issuance of a PIV Card to the
577 employee or contractor using the agency-approved pseudonym. The issuance of a PIV Card using an
578 authorized pseudonym shall follow the procedures in Section 2.8, PIV Card Issuance Requirements,
579 except that the card issuer must receive satisfactory evidence that the pseudonym is authorized by the
580 agency.

[5] See, for example, Section 10.5.7 of the Internal Revenue Service Manual (http://www.irs.gov/irm/index.html), which authorizes approval by an employee's supervisor of the use of a pseudonym to protect the employee's personal safety.

2.8.2 Grace Period

In some instances an individual's status as a Federal employee or contractor will lapse for a brief time period. For example, a Federal employee may leave one Federal agency for another Federal agency and thus occur a short employment lapse period, or an individual who was under contract to a Federal agency may receive a new contract from that agency shortly after the previous contract expired. In these instances, the card issuer may issue a new PIV Card without repeating the identity proofing and registration process if the issuer has access to the applicant's chain-of-trust record and the applicant can be reconnected to the chain-of-trust record.

When issuing a PIV Card under the grace period, the card issuer shall verify that PIV Card issuance has been authorized by a proper authority and that the employee's or contractor's background investigation is valid. Re-investigations shall be performed if required, in accordance with OPM guidance. At the time of issuance, the card issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. On successful match, the new PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide the two identity source documents (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new PIV Card.

2.9 PIV Card Maintenance Requirements

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

The data and credentials held by the PIV Card may need to be updated or invalidated prior to the expiration date of the card. The cardholder may change his or her name, retire, or change jobs; or the employment may be terminated, thus requiring invalidation of a previously issued card. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card maintenance. In order to maintain operational readiness of a cardholder's PIV Card, agencies may require PIV Card update, reissuance, or biometric enrollment more frequently than the maximum PIV Card and biometric lifetimes stated in this Standard. Shorter lifetimes may be specified by agency policy collectively, or on a case-by-case basis as sub-par operation is encountered.

2.9.1 PIV Card Renewal Requirements

Renewal is the process by which a valid PIV Card is replaced without the need to repeat the entire identity proofing and registration procedure. The renewal process may be used to replace a PIV Card that is nearing expiration or in the event of an employee status or attribute change. The entire identity proofing, registration, and issuance process, as described in Sections 2.7 and 2.8, shall be repeated if the issuer does not maintain a chain-of-trust record for the cardholder or if the renewal process was not started before the original PIV Card expired.

The renewal process for a PIV Card starts when a proper authority authorizes renewal of the credential. The issuer shall verify that the employee's or contractor's background investigation is valid before renewing the card and associated credentials. Re-investigations shall be performed if required, in accordance with OPM guidance.

The issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data that are available. Minimum accuracy requirements for the biometric match are specified in [SP 800-76].

On successful match, the new PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide the original PIV Card and another primary identity source document (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new PIV Card.

Prior to receiving the new PIV Card, the cardholder shall surrender the original PIV Card, which shall be collected and destroyed when the new PIV Card is issued.

If there is any data change about the cardholder, the issuer will record this in the chain-of-trust, if applicable. If the changed data is the cardholder's name, then the issuer shall meet the requirements in Section 2.9.1.1, Special Rule for Name Change by Cardholder.

Previously collected biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than 12 years after the date that the biometric data was obtained. As biometric authentication accuracy degrades with the time elapsed since initial collection, issuers may elect to refresh the biometric data after reconnecting the applicant to their chain-of-trust. Even if the same biometric data is reused with the new PIV Card, the digital signature must be recomputed with the new FASC-N and UUID.

A new PIV Authentication certificate and a new Card Authentication certificate shall be generated. The corresponding certificates shall be populated with the new FASC-N and UUID. For cardholders who are required to have a digital signature certificate, a new digital signature certificate shall also be generated. Key management key(s) and certificate(s) may be imported to the new PIV Card.

2.9.1.1 Special Rule for Name Change by Cardholder

Name changes frequently occur as a result of marriage, divorce, or as a matter of personal preference. In the event that a cardholder notifies a card issuer that his or her name has changed, and presents the card issuer with evidence of a formal name change, such as a marriage certificate, a divorce decree, judicial recognition of a name change, or other mechanism permitted by State law or regulation, the card issuer shall issue the cardholder a new card following the procedures set out in Section 2.9.1, PIV Card Renewal Requirements. If the expiration date of the new card is no later than the expiration date of the original PIV Card and no data about the cardholder, other than the cardholder's name, is being changed, then the new PIV Card may be issued without obtaining the approval of a proper authority and without performing a re-investigation.

2.9.2 PIV Card Reissuance Requirements

Reissuance is the process by which a PIV Card that has been compromised, lost, stolen, or damaged is replaced by a new PIV Card without the need to repeat the entire identity proofing and registration procedure. The cardholder can also apply for reissuance of a valid PIV Card if one or more logical credentials have been compromised. The entire identity proofing, registration, and issuance process, as described in Sections 2.7 and 2.8, shall be repeated if the issuer does not maintain a chain-of-trust record for the cardholder or if the cardholder did not apply for reissuance before the original PIV Card expired.

In case of reissuance, the card issuer shall verify that the employee's or contractor's background investigation is valid before reissuing the card and associated credentials.

The issuer shall perform a 1:1 biometric match of the applicant to reconnect to the chain-of-trust. The 1:1 biometric match requires either a match of fingerprint(s) or, if unavailable, other optional biometric data

held in the chain-of-trust (see Section 2.6). Minimum accuracy requirements for the biometric match are specified in [SP 800-76]. On successful match, the new PIV Card shall be released to the applicant. If the match is unsuccessful, or if no biometric data is available, the cardholder shall provide two identity source documents (as specified in Section 2.7), and an attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the new card.

When reissuing a PIV Card, normal revocation procedures must be in place for the compromised, lost, stolen, or damaged card to ensure the following:

- The PIV Card itself is revoked. Any local databases that contain FASC-N or UUID values must be updated to reflect the change in status.

- The certification authority (CA) shall be informed and the certificates corresponding to the PIV Authentication key and asymmetric Card Authentication key on the PIV Card shall be revoked. If present, the certificates corresponding to the digital signature key and the key management key shall also be revoked.

The PIV Card shall be collected and destroyed if possible. In the case of a lost, stolen, or compromised card, normal revocation procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures must be executed to disseminate the information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.

If the expiration date of the reissued PIV Card is later than the expiration date of the old card, the card issuer shall ensure that a proper authority has authorized reissuance of the credential, and that a re-investigation is performed if required, in accordance with OPM guidance. The same biometric data may be reused with the new PIV Card if the expiration date of the new PIV Card is no later than 12 years after the date that the biometric data was obtained.

2.9.3 PIV Card Post Issuance Update Requirements

A PIV Card post issuance update may be performed without replacing the PIV Card in cases where none of the printed information on the surface of the card is changed. The post issuance update applies to cases where one or more certificates, keys, biometric data objects, or signed data objects are updated. A post issuance update shall not modify the PIV Card expiration date, FASC-N, or UUID.

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

- Communication between the PIV Card issuer and the PIV Card shall occur only over mutually authenticated secure sessions between tested and validated cryptographic modules (one being the PIV Card).

- Data transmitted between the PIV Card issuer and PIV Card shall be encrypted and contain data integrity checks.

- The PIV Card Application will communicate with no end point entity other than the PIV Card issuer during the remote post issuance update.

Post issuance updates to biometric data objects, other than to the digital signature blocks within the biometric data objects, shall satisfy the requirements for verification data reset specified in Section 2.9.4.

If the PIV Authentication key, asymmetric Card Authentication key, the digital signature key, or the key management key, was compromised, the corresponding certificate shall be revoked.

2.9.4 PIV Card Verification Data Reset

The Personal Identification Number (PIN) on a PIV Card may need to be reset if the cardholder has forgotten the PIN or if PIN-based cardholder authentication has been disabled from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency.[6] PIN reset may be performed in-person at the issuer's facility, at an unattended kiosk operated by the issuer, or remotely via a general computing platform:

+ When PIN reset is performed in-person at the issuer's facility, the issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card, through either an on-card or off-card 1:1 biometric match, before providing the reset PIV Card back to the cardholder. In cases where a biometric match is not possible, the cardholder shall provide the PIV Card to be reset and another primary identity source document (as specified in Section 2.7). An attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the card.

+ PIN reset at an unattended issuer-operated kiosk shall ensure that the cardholder's biometric matches the stored biometric on the PIV Card, through either an on-card or off-card 1:1 biometric match, and that the PIV Card is authenticated. If the biometric match or card authentication is unsuccessful, the kiosk shall not reset the PIV Card.

+ Remote PIN reset on a general computing platform (e.g., desktop, laptop) shall only be performed if the following requirements are met:

    - the cardholder initiates a PIN reset with the issuer operator;
    - the operator authenticates the owner of the PIV Card through an out-of-band authentication procedure (e.g., pre-registered knowledge tokens); and
    - the cardholder's biometric matches the stored biometric on the PIV Card through a 1:1 on-card biometric comparison.

  The remote PIN reset operation shall satisfy the requirements for remote post issuance updates specified in Section 2.9.3.

Departments and agencies may adopt more stringent procedures for PIN reset (including disallowing PIN reset). PIN reset procedures shall be formally documented by each department and agency.

Verification data other than the PIN may also be reset (i.e., re-enrollment) by the card issuer. Before the reset, the issuer shall perform a 1:1 biometric match of the cardholder to reconnect to the chain-of-trust. The type of biometric used for the match shall not be the same as the type of biometric data that is being reset. For example, if fingerprint templates for on-card comparison are being reset, then a 1:1 iris match could be used to reconnect to the chain-of-trust. If no alternative biometric data is available, the cardholder shall provide the PIV Card to be reset and another primary identity source document (as

[6] Cardholders may change their PINs anytime by providing the current PIN and the new PIN values.

specified in Section 2.7). An attending operator shall inspect these and compare the cardholder with the facial image retrieved from the enrollment data record and the facial image printed on the PIV Card.

New verification reference data shall be enrolled. The PIV Card's activation methods associated with the verification data shall be reset and the new verification data shall be stored on the card.

Departments and agencies may adopt more stringent procedures for verification data reset (including disallowing verification data reset); such procedures shall be formally documented by each department and agency.

2.9.5 PIV Card Termination Requirements

The PIV Card shall be terminated under the following circumstances:

- a Federal employee separates (voluntarily or involuntarily) from Federal service;
- an employee of a Federal contractor separates (voluntarily or involuntarily) from his or her employer;
- a contractor changes positions and no longer needs access to Federal buildings or systems;
- a cardholder is determined to hold a fraudulent identity; or
- 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 shall be collected and destroyed, if possible.
- The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N or UUID values must be updated to reflect the change in status.
- The CA shall be informed and the certificates corresponding to PIV Authentication key and the asymmetric Card Authentication key on the PIV Card shall be revoked. If the PIV Card cannot be collected, the certificates corresponding to the digital signature and key management keys shall also be revoked, if present. If the PIV Card is collected and destroyed, then revocation of the certificates corresponding to the digital signature and key management keys is optional.
- The PII collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.

If the card cannot be collected, normal termination procedures shall be completed within 18 hours of notification. In certain cases, 18 hours is an unacceptable delay and in those cases emergency procedures must be executed to disseminate the information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.

2.10 PIV Derived Credentials Issuance Requirements

A valid PIV Card may be used as the basis for issuing a PIV derived credential in accordance with NIST Special Publication 800-157, *Guidelines for Personal Identity Verification (PIV) Derived Credentials*

[SP 800-157]. When a cardholder's PIV Card is terminated as specified in Section 2.9.5, any PIV derived credentials issued to the cardholder shall also be terminated.

2.11 PIV Privacy Requirements

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

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

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

- Assign an individual to the role of privacy official.[7] The privacy official is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the Standard. The individual serving in this role shall not assume any other operational role in the PIV system.

- Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing PII for the purpose of implementing PIV, consistent with the methodology of [E-Gov] and the requirements of [OMB0322]. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.

- Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, PII), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. Provide PIV applicants full disclosure of the intended uses of the information associated with the PIV Card and the related privacy implications.

- Assure that systems that contain PII for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY].

- Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.

- Ensure that only personnel with a legitimate need for access to PII in the PIV system are authorized to access the PII, including but not limited to information and databases maintained for registration and credential issuance.[8]

[7] Privacy official refers to the Senior Agency Official for Privacy (SAOP) or Chief Privacy Officer (CPO).
[8] Agencies may refer to NIST SP 800-122 [SP 800-122], *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*, for a best practice guideline on protection of PII.

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

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

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

- Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of PII. Specifically, employees may choose to use an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV Card.

3. PIV System Overview

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 authentication mechanisms that can be used consistently across departments and agencies. The authenticated identity information can then be used as a basis for access control in various Federal physical and logical access environments. The following sections briefly discuss the functional components of the PIV system and the lifecycle activities of the PIV Card.

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 PIN input device. The PIV cardholder interacts with these components to gain physical or logical access to the desired Federal resource.

+ **PIV Card Issuance and Management Subsystem**—the components responsible for identity proofing and registration, card and key issuance and management, and the various repositories and services (e.g., public key infrastructure (PKI) directory, certificate status servers) required as part of the verification infrastructure.

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

The PIV relying subsystem becomes relevant when the PIV Card is used to authenticate a cardholder who is seeking access to a physical or logical resource. Although this Standard does not provide technical specifications for this subsystem, various mechanisms for identification and authentication are defined in Section 6 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. The boundary shown in the figure is not meant to preclude FIPS 201 requirements on systems outside these boundaries.

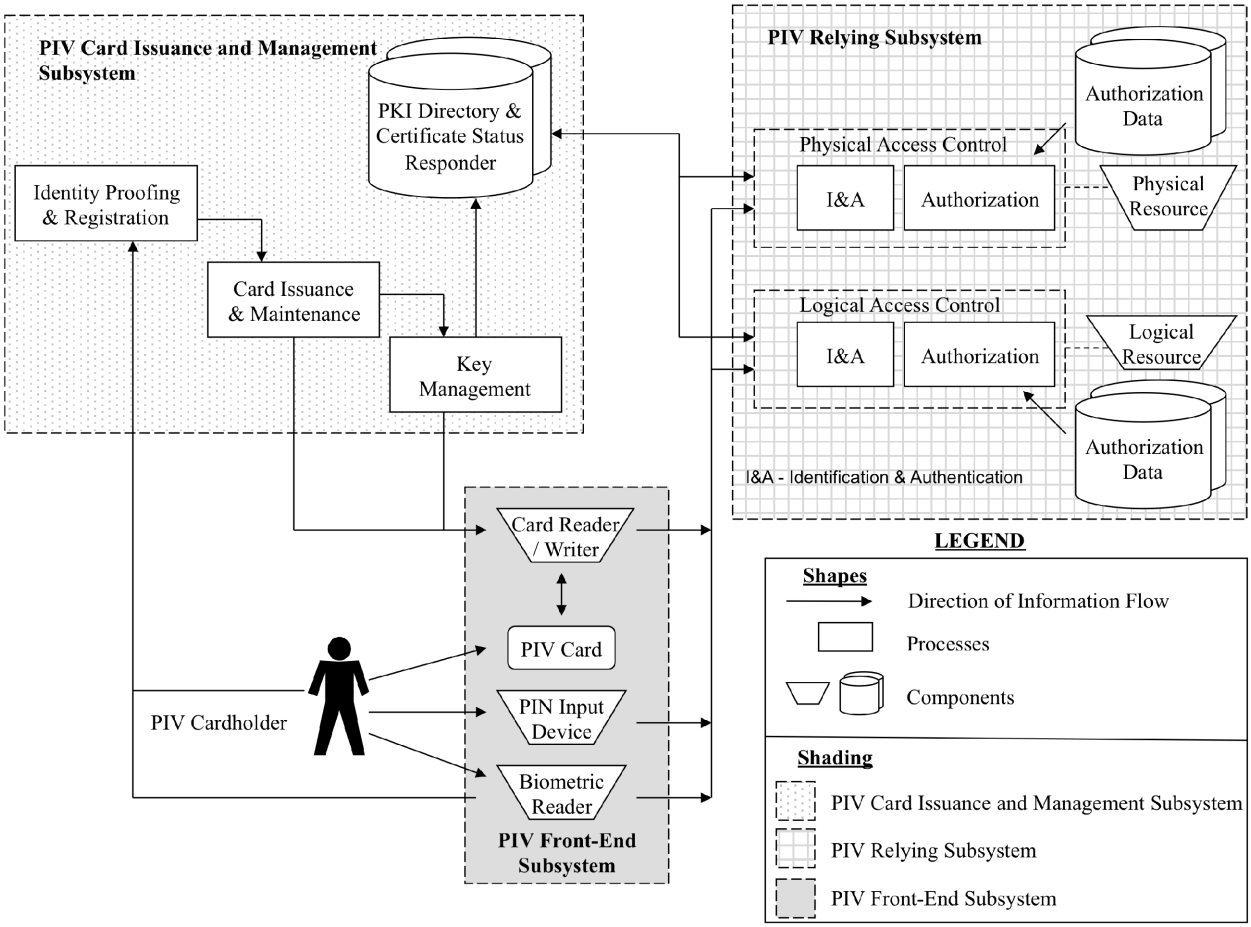


Figure 3-1. PIV System Notional Model

3.1.1 PIV Front-End Subsystem

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

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

Card writers, which are very similar to the card readers, personalize and initialize the information stored on PIV Cards. Card writers may also be used to perform remote PIV Card updates (see Section 2.9.3). The data to be stored on PIV Cards includes personal information, certificates, cryptographic keys, the PIN, and biometric data, and is discussed in further detail in subsequent sections.

PIN input devices can be used along with card readers when a higher level of authentication assurance is required. The cardholder presenting the PIV Card must type in his or her PIN into the PIN input device. For physical access, the PIN is typically entered using a PIN pad device; a keyboard is generally used for

logical access. The input of a PIN provides a "something you know"[9] authentication factor that activates[10] the PIV Card and enables access to other credentials resident on the card that provide additional factors of authentication. A cryptographic key and certificate, for example, provides an additional authentication factor of "something you have" (i.e., the card) through PKI-based authentication.

Biometric readers may be located at secure locations where a cardholder may want to gain access. These readers depend upon the use of biometric data of the cardholder, stored in the memory of the card, and its comparison with a real-time biometric sample. The use of biometrics provides an additional factor of authentication ("something you are") in addition to entering the PIN ("something you know") and providing the card ("something you have") for cryptographic key-based authentication ("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 printing photographs, names, and other information on the card and loading the relevant card applications, biometrics, and other data.

The key management component is responsible for the generation of key pairs, the issuance and distribution of digital certificates containing the public keys of the cardholder, and management and dissemination of certificate status information. The key management component is used throughout the lifecycle of PIV Cards—from generation and loading of authentication keys and PKI credentials, to usage of these keys for secure operations, to eventual 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 PIV Relying Subsystem

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

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

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

[9] For more information on the terms "something you know," "something you have," and "something you are," see [SP 800-63].
[10] Alternatively, on-card biometric comparison can be used to activate the PIV Card.

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

3.2 PIV Card Lifecycle Activities

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

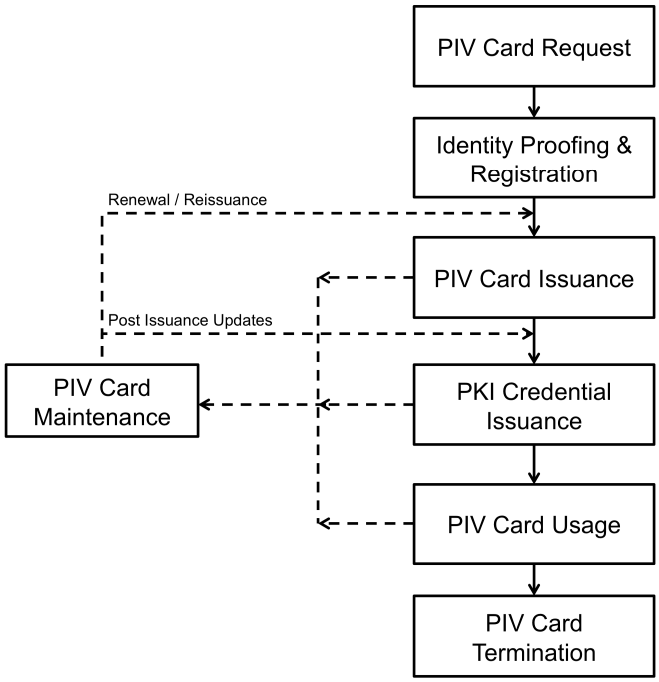


Figure 3-2. PIV Card Lifecycle Activities

Descriptions of the seven card lifecycle activities are as follows:

- **PIV Card Request.** This activity applies to the initiation of a request for the issuance of a PIV Card to an applicant and the validation of this request.

- **Identity Proofing and Registration.** The goal of this activity is to verify the claimed identity of the applicant, verify that the entire set of identity source documents presented at the time of registration is valid, capture biometrics, and optionally create the chain-of-trust record.

- **PIV Card Issuance.** This activity deals with the personalization (physical and logical) of the card and the issuance of the card to the intended applicant.

- **PKI Credential Issuance.** This activity deals with generating logical credentials and loading them onto the PIV Card.

934 + **PIV Card Usage.** During this activity, the PIV Card is used to perform cardholder authentication for
935 access to a physical or logical resource. Access authorization decisions are made after successful
936 cardholder identification and authentication.

937 + **PIV Card Maintenance.** This activity deals with the maintenance or update of the physical card and
938 the data stored thereon. Such data includes various card applications, PINs, PKI credentials, and
939 biometrics.

940 + **PIV Card Termination.** The termination process is used to permanently destroy or invalidate the
941 PIV Card and the data and keys needed for authentication so as to prevent any future use of the card
942 for 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 card specifications. Section 4.2 provides the logical card specifications. Section 4.3 specifies the requirements for card activation. Section 4.4 provides requirements for PIV Card readers.

4.1 PIV Card Physical Characteristics

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

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

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

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; and
- watermarks.

Incorporation of security features shall—

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

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

4.1.3 Physical Characteristics and Durability

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

- The PIV Card shall contain a contact and a contactless ICC interface.
- The card body shall be white in accordance with color representation in Section 4.1.5. Only a security feature, as described in Section 4.1.2, may modify the perceived color slightly. Presence of a security feature shall not prevent the recognition of white as the principal card body color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.
- The card body structure shall consist of card material(s) that satisfy the card characteristics in [ISO7810] and test methods in American National Standards Institute (ANSI) 322 [ANSI322]. Although the [ANSI322] test methods do not currently specify compliance requirements, the tests shall be used to evaluate card material durability and performance. The [ANSI322] tests minimally shall include card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet light exposure, and a laundry test. Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture.
- The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect 2000 hours of southwestern United States' sunlight exposure in accordance with [ISO10373], Section 5.12. Concentrated sunlight exposure shall be performed in accordance with [G90-98] and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading resistance and subjected to the same [ISO10373] dynamic bending test.
- There are methods by which proper card orientation can be indicated. Section 4.1.4.3, for example, defines Zones 21F and 22F, where card orientation features may be applied.[11] Note: If an agency determines that tactilely discernible markers for PIV Cards imposes an undue burden, the agency must implement policies and procedures to accommodate employees and contractors with disabilities in accordance with Sections 501 and 504 of the Rehabilitation Act.
- The card shall be 27- to 33-mil thick (before lamination) in accordance with [ISO7810].

[11] For some individuals, the contact surface for the ICC may be sufficient for determining the orientation of the card.

- The PIV Card shall not be embossed.

- Decals shall not be adhered to the card.

- Departments and agencies may choose to punch an opening in the card body to enable the card to be oriented by touch or to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted. Departments and agencies are strongly encouraged to ensure such alterations do not—

  - compromise card body durability requirements and characteristics;
  - invalidate card manufacturer warranties or other product claims;
  - alter or interfere with printed information, including the photo; or
  - damage or interfere with machine-readable technology, such as the embedded antenna.

- The card material shall withstand the effects of temperatures required by the application of a polyester laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer shall not interfere with the smart card reader operation. The card material shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.

The PIV Card may be subjected to additional testing.

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 4.2.

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

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

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

Because technological developments may obviate the need to have a restricted area, or change the size of the restricted area, departments and agencies are encouraged to work closely with card vendors and

manufacturers to ensure current printing procedures and methods are applied as well as potential integration of features that may improve tamper resistance and anti-counterfeiting of the PIV Card.

4.1.4.1 Mandatory Items on the Front of the PIV Card

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

Zone 2F—Name. The full name[12] shall be printed directly under the photograph in capital letters. The full name shall be composed of a Primary Identifier (i.e., surnames or family names) and a Secondary Identifier (i.e., pre-names or given names). The printed name shall match the name on the identity source documents provided during identity proofing and registration to the extent possible. The full name shall be printed in the <Primary Identifier>, <Secondary Identifier> format. The entire full name should be printed on available lines of Zone 2F and either identifier could be wrapped. The wrapped identifier shall be indicated with ">" character at the end of the line. The identifiers may be printed on separate lines if each fits on one line. Departments and agencies shall use the largest font size of 7 to 10 points that allows the full name to be printed. The font size 7 point allows space for 3 lines and shall only be used if the full name is greater than 45 characters. Table 4-1 provides examples of separate Primary and Secondary Identifier lines, single line with identifiers, wrapped full names, and full name in three lines. Note that the truncation should only occur if the full name cannot be printed in 7 point font.

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

Table 4-1. Name Examples

Name: John Doe Characteristics: simple full name of individual who does not have a middle name, two lines sufficient with 10 points.	**DOE,** **JOHN** Ⓖ
Name: Anna Maria Eriksson Characteristics: simple full name, two lines sufficient with 10 points.	**ERIKSSON,** **ANNA MARIA** Ⓖ
Name: Anna Maria Eriksson Characteristics: simple full name with abbreviated middle name, two lines sufficient with 10 points.	**ERIKSSON,** **ANNA M.** Ⓖ

[12] Alternatively, an authorized pseudonym as provided under the law as discussed in Section 2.8.1.

Name: Anna Maria Eriksson Characteristics: simple full name, one line sufficient for full name with 10 points.	ERIKSSON, ANNA MARIA G
Name: Susie Margaret Smith-Jones Characteristics: longer full name in two lines, sufficient space in 10 points.	SMITH-JONES, SUSIE MARGARET G
Name: Susie Margaret Smith-Jones Characteristics: longer full name wrapped, two lines sufficient with 10 points.	SMITH-JONES, SUSIE MA> RGARET G
Name: Chayapa Dejthamrong Krusuang Nilavadhanananda Characteristics: longer full name wrapped, two lines NOT sufficient with 10 points. Reduce the font size to 8 points.	NILAVADHANANANDA, CHAYA> PA DEJTHAMRONG KRUSUANG G
Name: Vaasa Silvaan Beenelong Wooloomooloo Warrandyte Warwarnambool Characteristics: longer full name, two lines NOT sufficient with 8 point, 7 point allows sufficient space for three lines in Zone 2F.	BEENELONG WOOLOOMOOLOO WARRANDYTE WARWARNAMBOOL, VAASA SILVAAN G
Name: Vaasa Silvaan Beenelong Wooloomooloo Warrandyte Warwarnambool Characteristics: same as previous but full name is wrapped.	BEENELONG WOOLOOMOOLOO W> ARRANDYTE WARWARNAMBOOL, V> AASA SILVAAN G
Name: Dingo Pontooroomooloo Vaasa Silvaan Beenelong Wooloomooloo Warrandyte Warwarnambool Characteristics: truncated full name, three lines with 7 point NOT sufficient.	BEENELONG WOOLOOMOOLOO W> ARRANDYTE WARWARNAMBOOL, D> INGO PONTOOROOMOOLOO VAASA G

Zone 8F—Employee Affiliation. An employee affiliation shall be printed on the card as depicted in Figure 4-1. Some examples of employee affiliation are "Employee," "Contractor," "Active Duty," and "Civilian."

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

Zone 14F—Card Expiration Date. The card expiration date shall be printed on the card as depicted in Figure 4-1. The card expiration date shall be in a YYYYMMMDD format whereby the MMM characters represent the three-letter month abbreviation as follows: JAN, FEB, MAR, APR, MAY, JUN, JUL, AUG, SEP, OCT, NOV, and DEC. The Zone 14F expiration date shall be printed in Arial 6 to 9 point bold.

Zone 15F—Color-Coding for Employee Affiliation. Color-coding shall be used for additional identification of employee affiliation as a background color for Zone 2F (name) as depicted in Figures 4-1 and 4-4. The following color scheme shall be used:

- Blue—Foreign National
- White—Government Employee
- Green—Contractor.

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

Zone 18F—Affiliation Color Code. The affiliation color code "B" for Blue, "W" for White, or "G" for Green shall be printed in a white circle in Zone 15F as depicted in Figure 4-1. The diameter of the circle shall not be more than 5 mm. Note that the lettering shall correspond to the printed color in Zone 15F.

Zone 19F—Card Expiration Date. The card expiration date shall be printed in a MMMYYYY format in the upper right-hand corner as depicted in Figure 4-1. The Zone 19F expiration date shall be printed in Arial 12pt Bold.

4.1.4.2 Mandatory Items on the Back of the PIV Card

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

Zone 2B—Issuer Identification Number. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, 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 PIV Card

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

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

Zone 4F—Agency Specific Text Area. If used, this area can be used for printing agency specific requirements, such as employee status, as shown in Figure 4-2.

Zone 5F—Rank. If used, the cardholder's rank shall be printed in the area as illustrated in Figure 4-2. Data format is at the department or agency's discretion.

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

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

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

Zone 12F—Footer. The footer is the location for the *Federal 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 white lettering on a red background. Departments and agencies may also use Zone 9F to further identify the Federal emergency respondent's official role. Some examples of official roles are "Law Enforcement," "Fire Fighter," and "Emergency Response Team (ERT)."

When Zone 15F indicates Foreign National affiliation and the department or agency does not need to highlight emergency response official status, Zone 12F may be used to denote the country or countries of citizenship. If so used, the department or agency shall print the country name or the three-letter country abbreviation (alpha-3 format) in accordance with ISO 3166-1, Country Codes [ISO3166]. Figure 4-4 illustrates an example of Foreign National color-coding using country abbreviations.

Zone 13F—Issue Date. If used, the card issuance date shall be printed above the expiration date in YYYYMMMDD format as depicted in Figure 4-3.

Zone 16F—Photo Border. 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 15F to enable departments and agencies to develop various employee categories. The photo border shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the department or agency's discretion.

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

Zone 20F—Organizational Affiliation Abbreviation. The organizational affiliation abbreviation may be printed in the upper right-hand corner below the Zone 19F expiration date as shown in Figure 4-2. If printed, the organizational affiliation abbreviation shall be printed in Arial 12pt Bold.

Zone 21F –Edge Ridging or Notched Corner Tactile Marker. If used, this area shall incorporate edge ridging or a notched corner to indicate card orientation as depicted in Figure 4-4. Departments and

agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted.

Zone 22F –Laser Engraving Tactile Marker. If used, tactilely discernible marks shall be created using laser engraving to indicate card orientation as depicted in Figure 4-4. There shall be an opening in the lamination foil where laser engraving is performed. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity and printing process is not adversely impacted.

4.1.4.4 Optional Items on the Back of the PIV Card

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

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

Zone 5B—Physical Characteristics of Cardholder. If used, the cardholder physical characteristics (e.g., height, eye color, hair color) shall be printed in the general area illustrated in Figure 4-7.

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

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

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

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

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

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

In the case of the Department of Defense, the back of the card will have a distinct appearance as depicted in Figure 4-8. This is necessary to display information required by the Geneva Accord and to facilitate legislatively mandated medical entitlements.

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

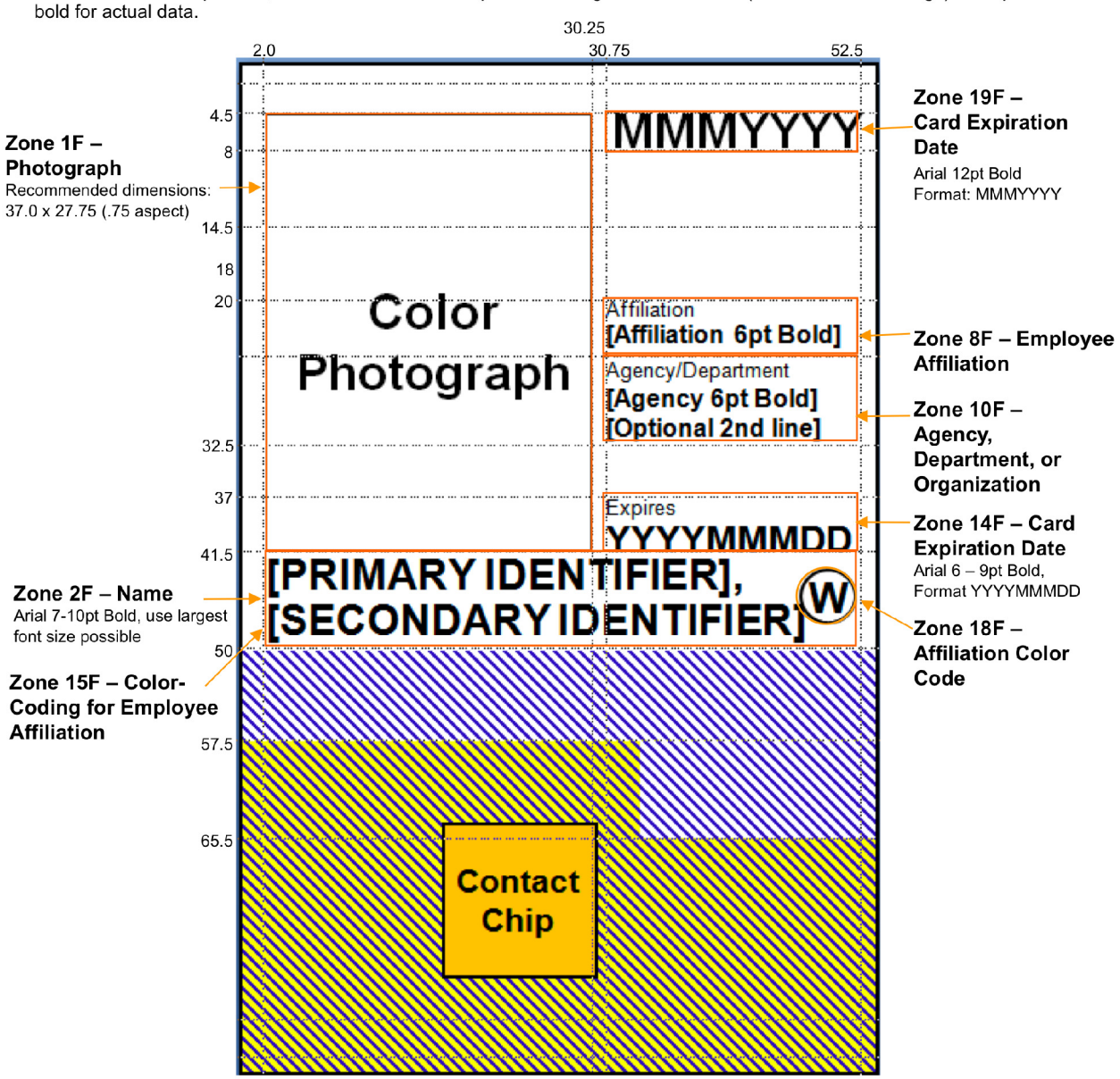


Figure 4-1. Card Front—Printable Areas and Required Data

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

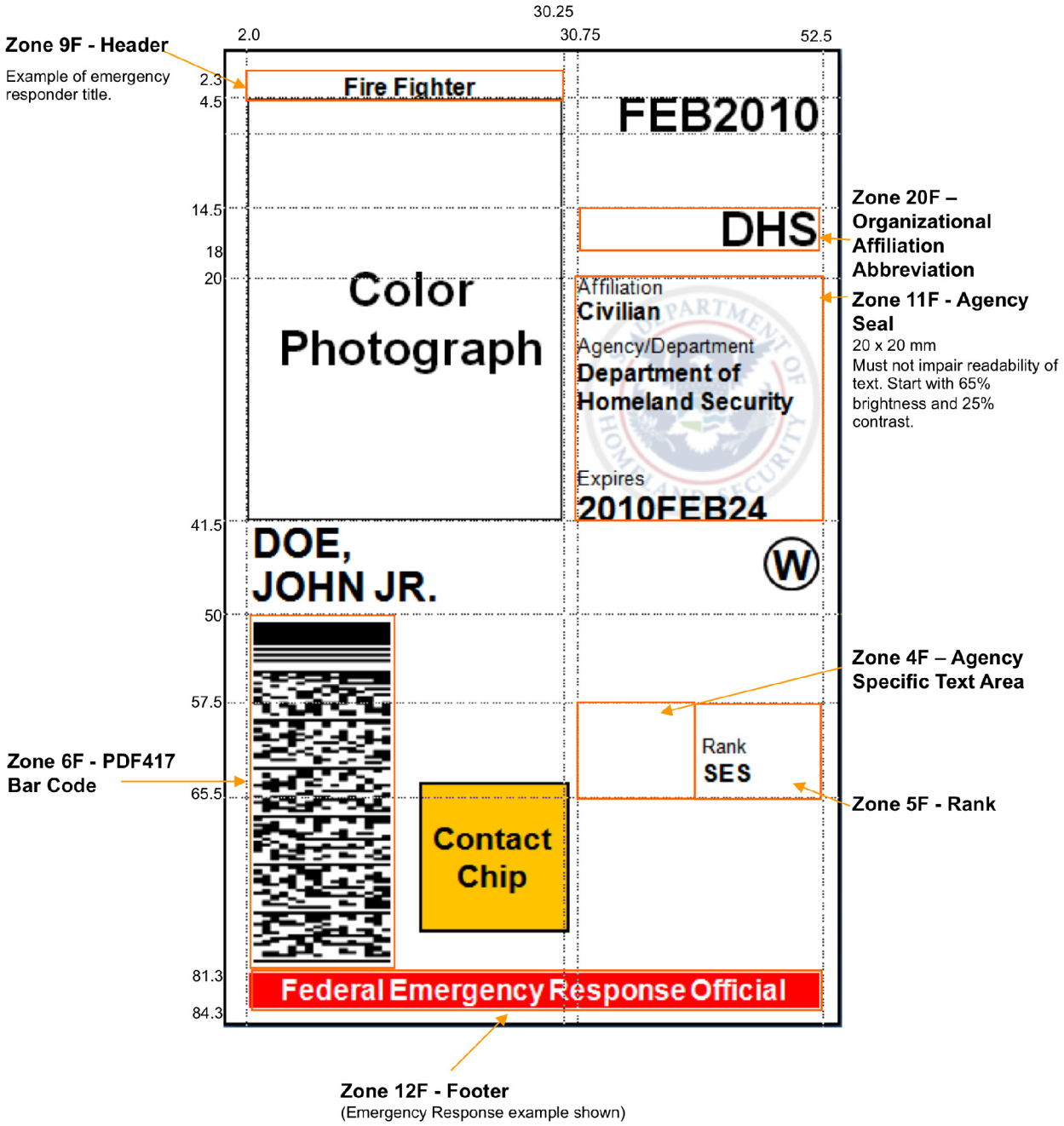


Figure 4-2. Card Front—Optional Data Placement—Example 1

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

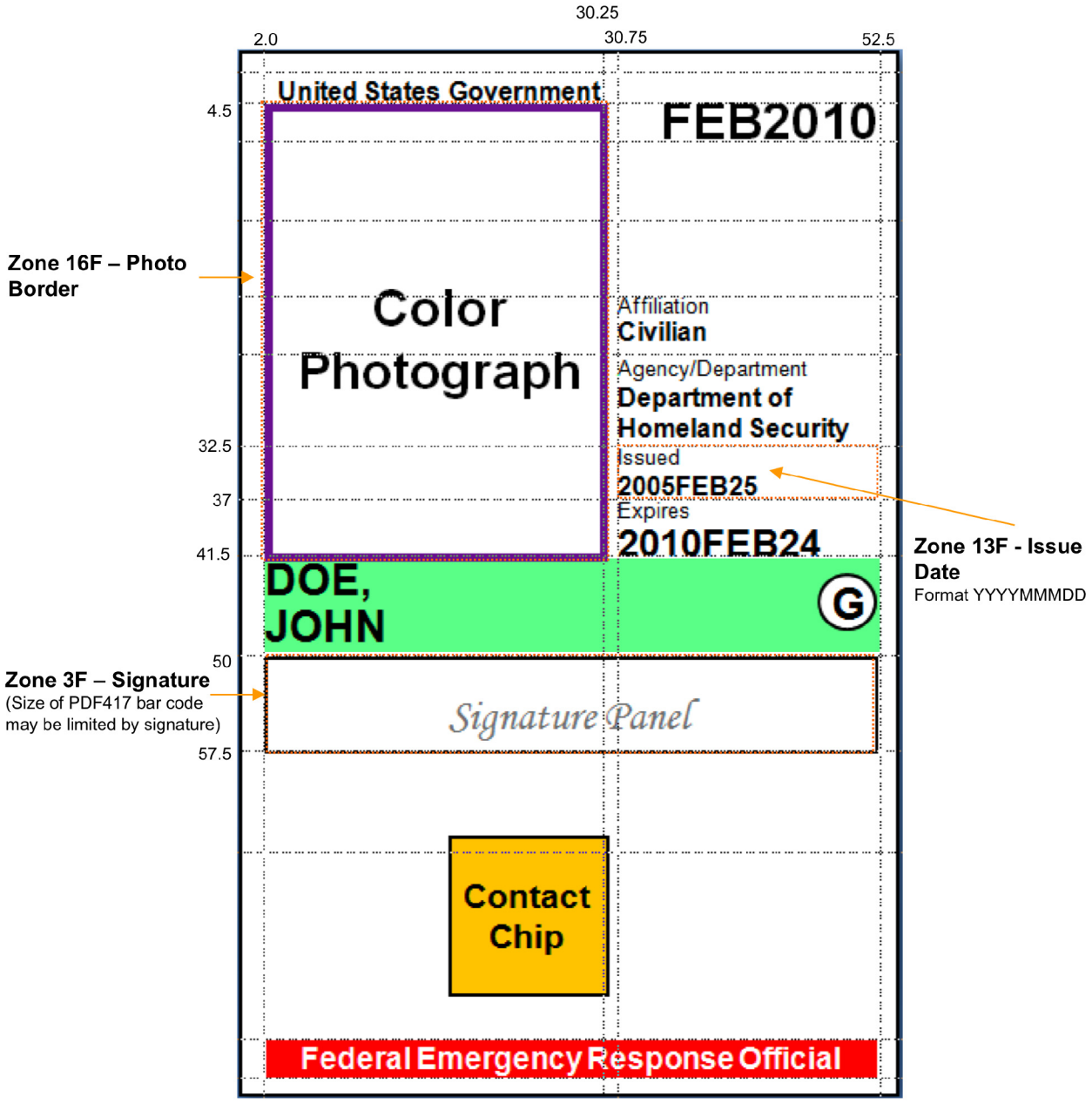


Figure 4-3. Card Front—Optional Data Placement—Example 2

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

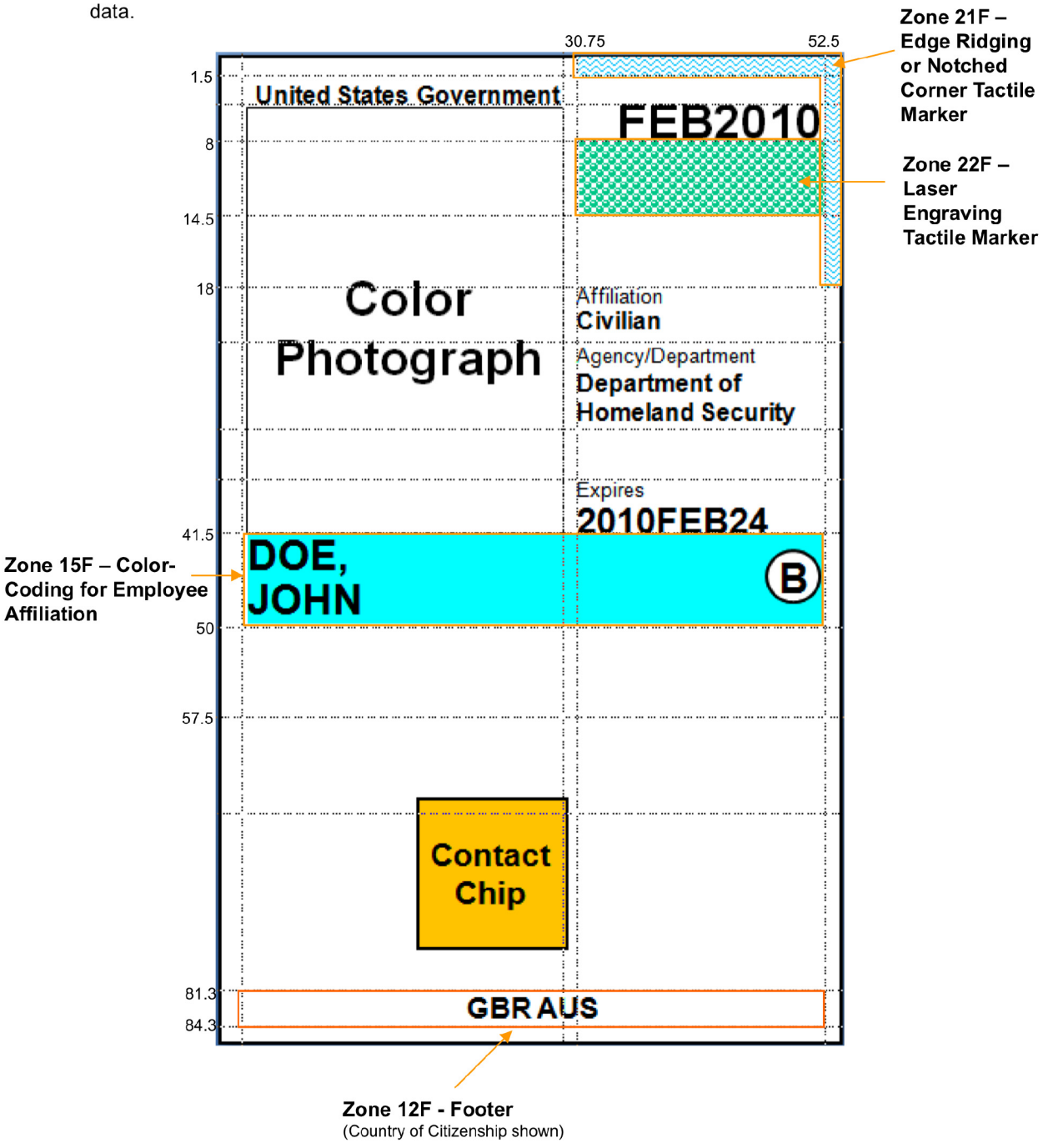


Figure 4-4. Card Front—Optional Data Placement—Example 3

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

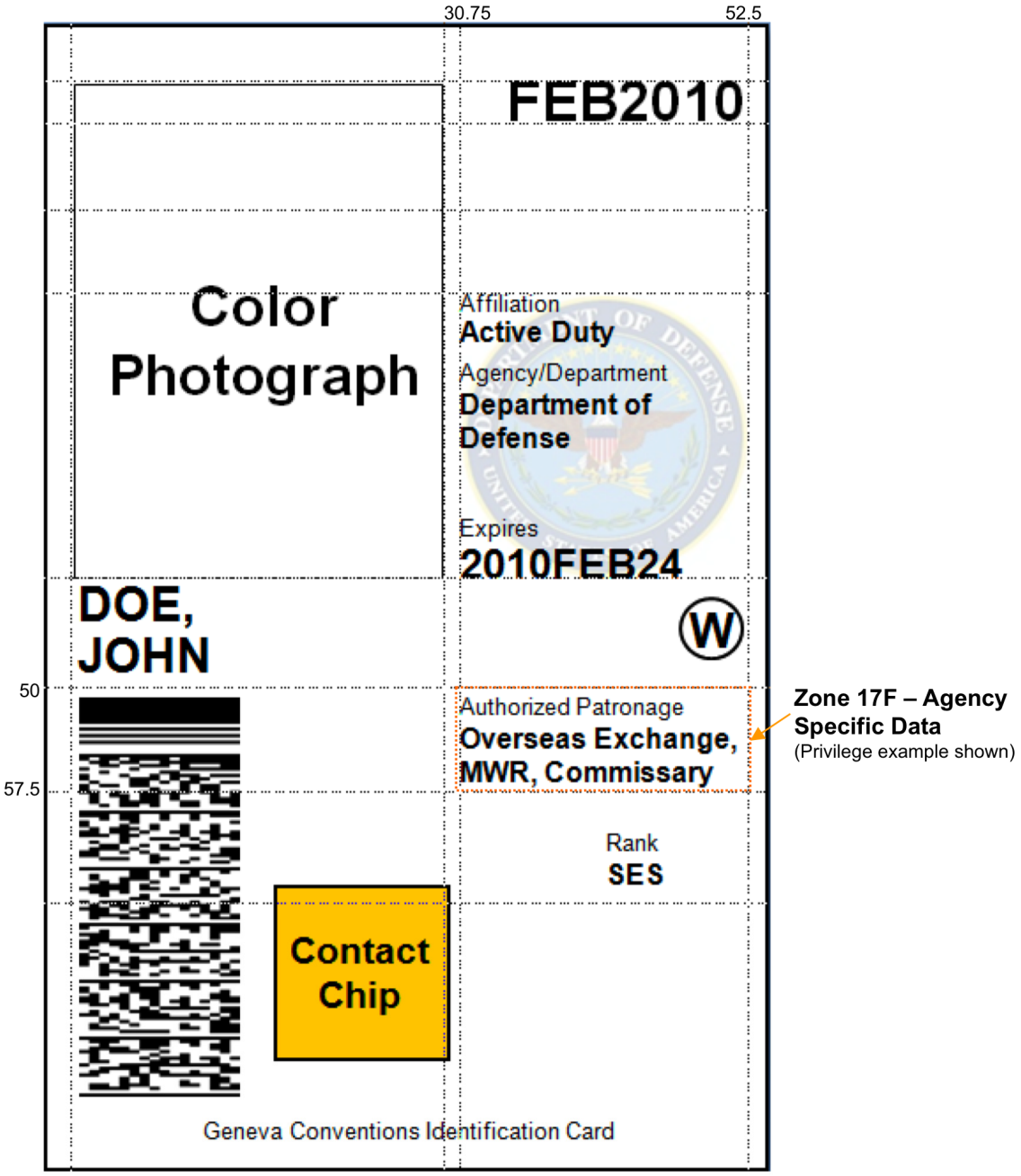
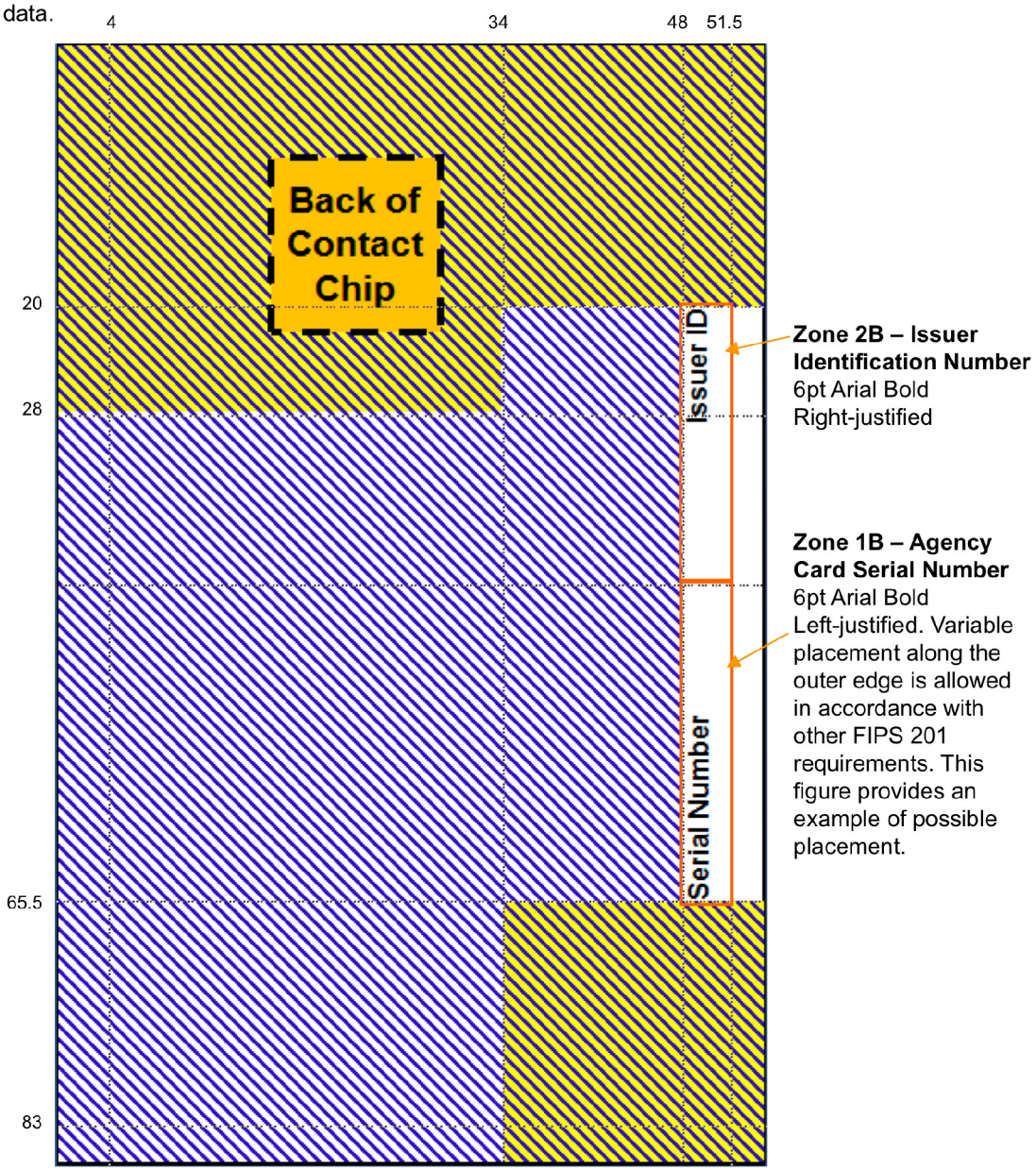


Figure 4-5. Card Front—Optional Data Placement—Example 4

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.

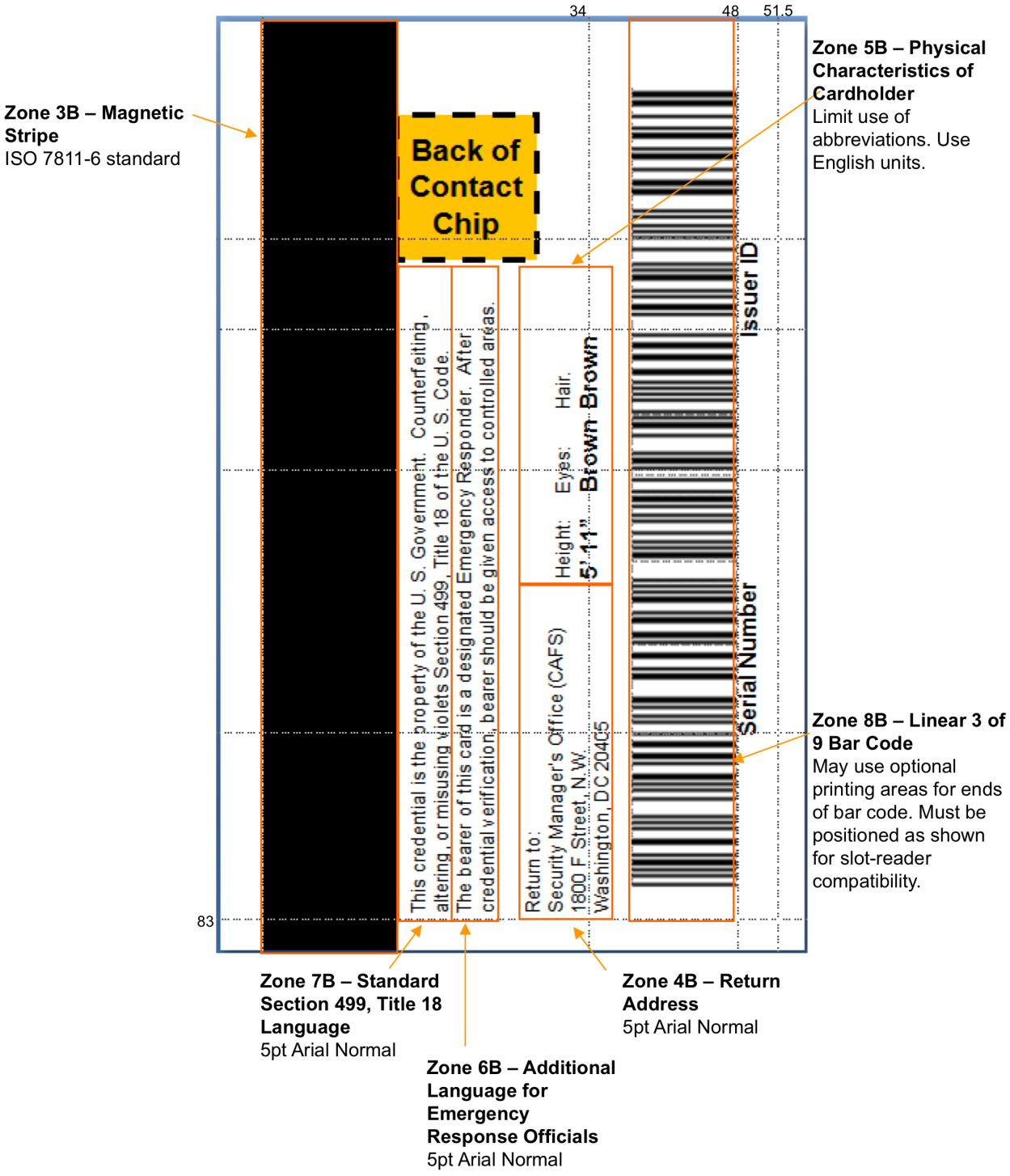
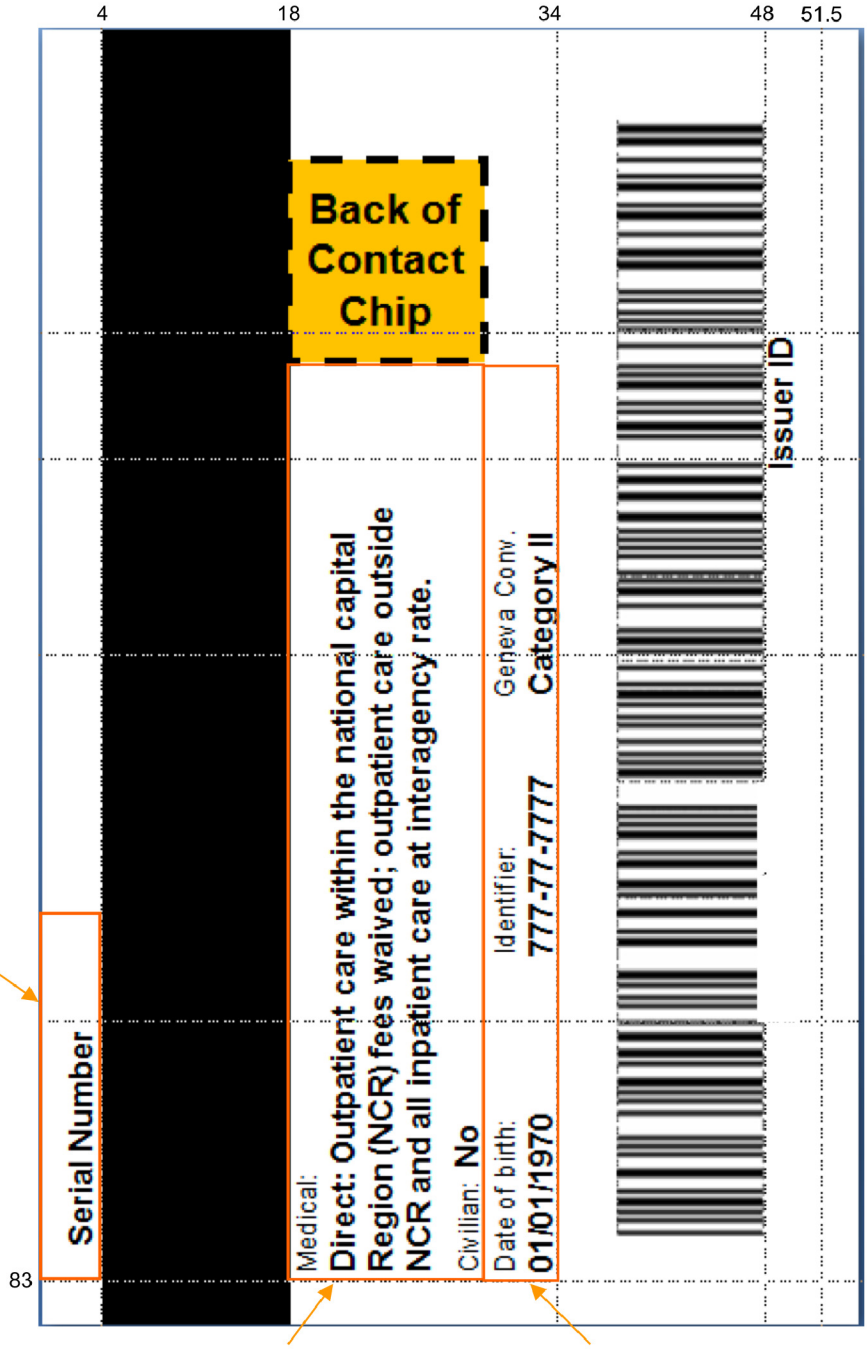


Figure 4-7. Card Back—Optional Data Placement—Example 1

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 1B – Agency Card Serial Number
6pt Arial Bold
Variable placement along the outer edge is allowed in accordance with other FIPS 201 requirements.

Zone 9B – Agency-Specific Text
Used instead of zones 6B & 7B (Medical example shown)

Zone 10B – Agency-Specific Text
Used instead of zones 4B & 5B (DOB, ID, Geneva example shown)

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

4.1.5 Color Representation

Table 4-2 provides quantitative specifications for colors in three different color systems: sRGB Tristimulus, sRGB ([IEC 61966], Color management – default RGB color space), and CMYK (Cyan, Magenta, Yellow and Key or 'blacK'). Since the card body is white, the white color-coding is achieved by the absence of printing. Note that presence of the security feature, which may overlap colored or printed regions, may modify the perceived color. In the case of colored regions, the effect of overlap shall not prevent the recognition of the principal color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.

Table 4-2. Color Representation

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

The colors in Table 4-2 can be mapped to the Pantone[13] color cue; however, note that this will not produce an exact match. An agency or department may use the following Pantone mappings in cases where Table 4-2 scales are not available.

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

4.2 PIV Card Logical Characteristics

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

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. The following mandatory data elements are part of the data model for PIV logical credentials that support authentication mechanisms interoperable across agencies:

- a PIN;
- a CHUID;
- PIV authentication data (one asymmetric key pair and corresponding certificate);

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

- two fingerprint templates;
- an electronic facial image; and
- card authentication data (one asymmetric key pair and corresponding certificate).

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

- an asymmetric key pair and corresponding certificate for digital signatures; and
- an asymmetric key pair and corresponding certificate for key management.

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

- one or two iris images;
- one or two fingerprint templates for on-card comparison;
- a symmetric Card Authentication key for supporting physical access applications; and
- a symmetric PIV Card Application Administration key associated with the card management system.

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

PIV logical credentials fall into the following three categories:

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

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

4.2.1 Cardholder Unique Identifier (CHUID)

The PIV Card shall include the CHUID as defined in [SP 800-73]. The CHUID includes the Federal Agency Smart Credential Number (FASC-N) and the Global Unique Identification Number (GUID), which uniquely identify each card as described in [SP 800-73]. The value of the GUID data element shall be a 16-byte binary representation of a valid Universally Unique IDentifier (UUID) [RFC4122]. The CHUID shall also include an expiration date data element in machine-readable format that specifies when the card expires. The expiration date format and encoding rules are as specified in [SP 800-73].

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

This Standard requires inclusion of the asymmetric signature field in the CHUID container. The asymmetric signature data element of the CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as specified in [SP 800-73]. Algorithm and key size requirements for the asymmetric signature and digest algorithm are detailed in [SP 800-78].

The public key required to verify the digital signature shall be provided in the *certificates* field of the CMS external digital signature in a content signing certificate, which shall be an X.509 digital signature certificate issued under the id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON].[14] The content signing certificate shall also include an extended key usage (*extKeyUsage)* extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix B.

4.2.2 Cryptographic Specifications

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

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

The PIV Card may include an asymmetric private key and corresponding public key certificate to establish symmetric keys for use with secure messaging, as specified in [SP 800-73] and [SP 800-78]. Secure messaging enables data and commands transmitted between the card and an external entity to be both integrity protected and encrypted. Secure messaging may be used, for example, to enable the use of on-card biometric comparison as an authentication mechanism.

Once secure messaging has been established, a *virtual contact interface* may be established. Requirements for the virtual contact interface are specified in [SP 800-73]. Any operation that may be performed over the contact interface of the PIV Card may also be performed over the virtual contact interface. With the exception of the *Card Authentication key* and keys used to establish a secure messaging, the cryptographic private key operations shall be performed only through the contact interface or the virtual contact interface.

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

The PIV Card has both mandatory keys and optional keys:

- The *PIV Authentication key* is a mandatory asymmetric private key that supports card and cardholder authentication for an interoperable environment.

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

- The *asymmetric Card Authentication key* is a mandatory private key that supports card authentication for an interoperable environment.

- The *symmetric (secret) Card Authentication key* supports card authentication for physical access, and it is optional.

- The *digital signature key* is an asymmetric private key supporting document signing.

- The *key management key* is an asymmetric private key supporting key establishment and transport. Optionally, up to twenty retired key management keys may also be stored on the PIV Card.

- The *PIV Card Application Administration Key* is a symmetric key used for personalization and post-issuance activities, and it is optional.

- The PIV Card may include additional key(s) for use with secure messaging. These keys are defined in [SP 800-73] or [SP 800-78].

All PIV cryptographic keys shall be generated within a [FIPS140] validated cryptographic module with overall validation at Level 2 or above. In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage. The scope of the validation for the PIV Card shall include all cryptographic operations performed over both the contact and contactless interfaces (1) by the PIV Card Application, (2) as part of secure messaging as specified in this section, and (3) as part of remote post issuance updates as specified in Section 2.9.3. Specific algorithm testing requirements for the cryptographic operations performed by the PIV Card Application are specified in [SP 800-78].

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

- **PIV Authentication Key.** This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV Authentication key. The cryptographic operations that use the PIV Authentication key shall be available only through the contact and the virtual contact interfaces of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

  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 X.509 certificate shall also include the UUID value from the GUID data element of the CHUID in the subject alternative name extension. The UUID shall be encoded as a uniform resource identifier (URI), as specified in Section 3 of [RFC4122]. The expiration date of the certificate must be no later than the expiration date of the PIV Card. The PIV Authentication certificate shall include a PIV NACI indicator (background investigation indicator) extension; this non-critical extension indicates the status of the subject's background investigation at the time of card issuance. Section 5 of this document specifies the certificate format and the key management infrastructure for the PIV Authentication key.

- **Asymmetric Card Authentication Key.** The asymmetric Card Authentication key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the Card Authentication key. Cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. Private key operations may be performed using this key without card activation (e.g., the PIN need not be supplied for operations with this key).

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 X.509 certificate shall also include the UUID value from the GUID data element of the CHUID in the subject alternative name extension. The UUID shall be encoded as a URI, as specified in Section 3 of [RFC4122]. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for asymmetric PIV Card Authentication keys.

\+ **Symmetric Card Authentication Key.** The symmetric Card Authentication key is imported onto the card by the issuer. The PIV Card shall not permit exportation of this key. If present, the symmetric Card Authentication key shall be unique for each PIV Card and shall meet the algorithm and key size requirements stated in [SP 800-78]. If present**,** cryptographic operations using this key may be performed without card activation (e.g., the PIN need not be supplied for operations with this key). The cryptographic operations that use the Card Authentication key shall be available through the contact and the contactless interfaces of the PIV Card. This Standard does not specify key management protocols or infrastructure requirements.

+ 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 and the virtual contact interfaces of the PIV Card. Private key operations may not be performed without explicit user action, as this Standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.[15]

The PIV Card shall store a corresponding X.509 certificate to support validation of the public key. The expiration date of the certificate must be no later than the expiration date of the PIV Card. Section 5 of this document specifies the certificate format and the key management infrastructure for PIV digital signature keys.

+ Key Management Key. This key may be generated on the PIV Card or imported to the card. If present, the cryptographic operations that use the key management key must only be accessible using the contact and the virtual contact interfaces of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation).

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

+ PIV Card Application Administration Key. The PIV Card Application Administration Key is imported onto the card by the issuer. If present, the cryptographic operations that use the PIV Card Application Administration Key must only be accessible using the contact interface of the PIV Card.

4.2.3 PIV Biometric Data Specifications

4.2.3.1 Biometric Data Representation

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

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

- Two fingerprint templates. If no fingerprint images meeting the quality criteria of [SP 800-76] are available, the PIV Card shall nevertheless be populated with fingerprint records as specified in [SP800-76].

- An electronic facial image.

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

- One or two iris images.

- Fingerprint templates for on-card comparison.[16]

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

4.2.3.2 Biometric Data Protection

The integrity of all biometric data, except for fingerprint templates for on-card comparison, shall be protected using digital signatures as follows. The records shall be prepended with a Common Biometric Exchange Formats Framework (CBEFF) header (referred to as CBEFF_HEADER) and appended with the CBEFF signature block (referred to as the CBEFF_SIGNATURE_BLOCK) [CBEFF].

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

The CBEFF_SIGNATURE_BLOCK contains the digital signature of the biometric data and thus facilitates the verification of integrity of the biometric data. The CBEFF_SIGNATURE_BLOCK shall be encoded as a CMS external digital signature as specified in [SP 800-76]. The algorithm and key size requirements for the digital signature and digest algorithm are detailed in [SP 800-78].

The public key required to verify the digital signature shall be contained in a content signing certificate, which shall be issued under the id-fpki-common-devicesHardware, id-fpki-common-hardware, or id-fpki-common-High policy of [COMMON].[17] The content signing certificate shall also include an extended key usage (*extKeyUsage)* extension asserting id-PIV-content-signing. If the signature on the biometric was generated with a different key than the signature on the CHUID, the *certificates* field of the CMS external digital signature shall include the content signing certificate required to verify the signature on the biometric. Otherwise, the *certificates* field shall be omitted. Additional descriptions for the PIV object identifiers are provided in Appendix B.

4.2.3.3 Biometric Data Access

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

- shall be readable through the contact interface and after the presentation of a valid PIN; and

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

[16] The on-card and off-card fingerprint reference data are stored separately and, as conformant instances of different formal fingerprint standards, are syntactically different. This is described more fully in [SP 800-76].

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

On-card biometric comparison may be performed over the contact and the contactless interfaces of the PIV Card to support card activation (Section 4.3.1) and cardholder authentication (Section 6.2.2). The fingerprint templates for on-card comparison shall not be exportable. If implemented, on-card biometric comparison shall be implemented and used in accordance with [SP 800-73] and [SP 800-76].

4.2.4 PIV Unique Identifiers

A cardholder is authenticated through identification and authentication (I&A) using the PIV credential (and its identifier) in authentication mechanisms described in Section 6. The authenticated identity may then be used as the basis for making authorization decisions. Unique identifiers for both authentication and authorization are provided in this Standard in order to uniquely identify the cardholder. The two types of identifiers that serve as identification (of the cardholder) for authentication and authorization purposes, are described as follows:

- Credential identifiers

  Each PIV card contains a UUID and a FASC-N that uniquely identify the card and, by correspondence, the cardholder. These two credential identifiers are represented in all of the authentication data elements for the purpose of binding the PIV data elements to the same PIV Card.

- Cardholder Identifiers

  Other identifiers may be present in credentials on the PIV Card that identity the cardholder rather than the card. Examples include the subject name and names that may appear in the subjectAltName extension in the PIV Authentication certificate.

4.3 PIV Card Activation

The PIV Card shall be activated[18] to perform privileged[19] operations such as using the PIV Authentication key, digital signature key, and key management key. The PIV Card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system. Cardholder activation is described in Section 4.3.1 and card management system activation is described in Section 4.3.2.

4.3.1 Activation by Cardholder

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

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

[18] Activation in this context refers to the unlocking of the PIV Card Application so privileged operations can be performed.
[19] A read of a CHUID or use of the Card Authentication key is not considered a privileged operation.

4.3.2 Activation by Card Management System

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

4.4 Card Reader Requirements

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

4.4.1 Contact Reader Requirements

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

4.4.2 Contactless Reader Requirements

Contactless card readers shall conform to [ISO14443] standard for the card-to-reader interface and data transmitted over the [ISO14443] link shall conform to [ISO7816]. In cases where these readers are connected to general-purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-host system interface. Specifically, the contactless card readers shall conform to the requirements specified in [SP 800-96]. In physical access control systems where the readers are not connected to general-purpose desktop computing systems, the reader-to-host system interface is not specified in this Standard. This is necessary to allow retrofitting of PIV readers into existing physical access control systems that use a variety of non-standard card reader communication interfaces.

4.4.3 Reader Resilience and Flexibility

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

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

4.4.4 Card Activation Device Requirements

When the PIV Card is used with OCC data or a PIN for physical access, the input device shall be integrated with the PIV Card reader. When the PIV Card is used with OCC data or a PIN for logical access (e.g., to authenticate to a Web site or other server), the input device is not required to be integrated with the PIV Card reader. If the input device is not integrated with the PIV Card reader, the OCC data or the PIN shall be transmitted securely and directly to the PIV Card for card activation.

The specifications for fingerprint capture devices for on-card comparison are given in [SP 800-76].

Malicious code could be introduced into the PIN capture and biometric reader devices for the purpose of compromising or otherwise exploiting the PIV Card. General good practice to mitigate malicious code threats is outside the scope of this document.[20]

[20] See SP 800-53, *Recommended Security Controls for Federal Information Systems and Organizations* [SP 800-53].

5. PIV Key Management Requirements

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

5.1 Architecture

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

5.2 PKI Certificate

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

5.2.1 X.509 Certificate Contents

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

- Certificates containing the public key associated with an asymmetric Card Authentication key shall conform to *Worksheet 8: Card Authentication Certificate Profile* in [PROF].

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

- Certificates containing the public key associated with a PIV Authentication private key shall conform to *Worksheet 9: PIV Authentication Certificate Profile* in [PROF].

- Certificates containing the public key associated with a key management private key shall conform to *Worksheet 6: Key Management Certificate Profile* in [PROF].[21]

- Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP 800-78].

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

5.3 X.509 CRL Contents

CAs that issue certificates corresponding to PIV private keys shall issue CRLs as specified in [COMMON]. The contents of X.509 CRLs shall conform to *Worksheet 4: CRL Profile* in [PROF].

5.4 Legacy PKIs

For the purposes of this Standard, legacy PKIs are the PKIs of departments and agencies that have cross-certified with the Federal Bridge CA (FBCA) at the Medium Hardware or High Assurance Level. Legacy PKIs that issue PIV Authentication certificates and Card Authentication certificates shall meet the requirements specified in Sections 5.2.1, 5.3, 5.5, 5.5.1, and 5.5.2, with respect to the PIV Authentication certificates and Card Authentication certificates that they issue. Departments and agencies may assert department or agency-specific policy object identifiers (OIDs) in PIV Authentication Certificates and Card Authentication Certificates in addition to the id-fpki-common-authentication policy OID and the id-fpki-common-cardAuth OID, respectively. This specification imposes no requirements on digital signature or key management certificates issued by legacy PKIs.

5.5 PKI Repository and OCSP Responder(s)

The PIV PKI repository and Online Certificate Status Protocol (OCSP) responder provides PIV Card and key status information across departments, agencies, and other organizations, to support high-assurance interagency PIV Card interoperation. Departments and agencies will be responsible for notifying CAs 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 certificates (PIV Authentication certificate and Card Authentication certificate) shall not be after the expiration date of the PIV Card. If the card is revoked, the authentication certificates shall be revoked. However, an authentication certificate (and its associated key pair) may be revoked without revoking the PIV Card and may then be replaced. The presence of a valid, unexpired, and unrevoked authentication certificate on a card is proof that the card was issued and is not revoked.

Because an authentication certificate typically is valid several years, a mechanism to distribute certificate status information is necessary. CRL and OCSP are the two commonly used mechanisms. CAs that issue authentication certificates shall maintain a Hypertext Transfer Protocol (HTTP) accessible web server that holds the CRLs for the certificates it issues, as well as any CA certificates issued to or by it, as specified in [PROF].

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

5.5.1 Certificate and CRL Distribution

This Standard requires distribution of CA certificates and CRLs using HTTP. Specific requirements are found in the Shared Service Provider Repository Service Requirements [SSP REP].

Certificates that contain the FASC-N or UUID in the subject alternative name extension, such as PIV Authentication certificates and Card Authentication certificates, shall not be distributed publicly (e.g., via the Lightweight Directory Access Protocol (LDAP) or HTTP accessible from the public Internet).

Individual departments and agencies can decide whether other user certificates (digital signature and key management) can be distributed via LDAP. When user certificates are distributed, the requirements in Table IV—End-Entity Certificate Repository Service Requirements of [SSP REP] shall be satisfied.

5.5.2 OCSP Status Responders

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

6. PIV Cardholder Authentication

This section defines a suite of authentication mechanisms that are supported by all the PIV Cards, and their applicability in meeting the requirements for a set of graduated levels of identity assurance. This section also defines some authentication mechanisms that make use of credential elements that may optionally be included on PIV Cards. Specific implementation details of authentication mechanisms identified in this section are provided in [SP 800-73]. Moreover, while a wide range of authentication mechanisms is identified in this section, departments and agencies may adopt additional mechanisms that use the identity credentials on the PIV Card. In the context of the PIV Card Application, identity authentication is defined as the process of establishing confidence in the identity of the cardholder presenting a PIV Card. The authenticated identity can then be used to determine the permissions or authorizations granted to that identity for access to various physical and logical resources.

6.1 PIV Assurance Levels

This Standard defines four levels of assurance for identity authentication supported by the PIV Card Application. Each assurance level sets a degree of confidence established in the identity of the holder of the PIV Card. The entity performing the authentication establishes confidence in the identity of the PIV cardholder through the following:

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

2) the security of the PIV Card issuance and maintenance processes; and

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

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

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

Parties responsible for controlling access to Federal resources (both physical and logical) shall determine the appropriate level of identity assurance required for access, based on the harm and impact to individuals and organizations as a result of errors in the authentication of the identity of the PIV cardholder. Once the required level of assurance has been determined, the authentication mechanisms specified within this section may be applied to achieve the required degree of confidence in the identity of the PIV cardholder.

6.1.1 Relationship to OMB's E-Authentication Guidance

The levels of identity authentication assurance defined within this Standard are closely aligned with Section 2 of OMB's E-Authentication Guidance for Federal Agencies, M-04-04 [OMB0404]. Specifically, Table 6-1 shows the notional relationship between the PIV assurance levels and the M-04-04 E-Authentication assurance levels.

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

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

[OMB0404] addresses "four levels of identity assurance for electronic transactions requiring authentication" and prescribes a methodology for determining the level of identity assurance required based on the risks and potential impacts of errors in identity authentication. In the context of the PIV Card, owners of logical resources shall apply the methodology defined in [OMB0404] to identify the level of identity authentication assurance required for their electronic transaction. Parties that are responsible for access to physical resources may use a methodology similar to that defined in [OMB0404] 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 credential set hosted by the PIV Card Application. PIV Cards can be used for identity authentication in environments that are equipped with card readers as well as those that lack card readers. Card readers, when present, can be contact readers or contactless readers. The usage environment affects the PIV authentication mechanisms that may be applied to a particular situation.

6.2.1 Authentication Using Off-Card Biometric Comparison

The PIV Card Application hosts the signed fingerprint templates and, optionally, the signed iris images. Either biometric can be read from the card following cardholder-to-card (CTC) authentication using a PIN supplied by the cardholder. These PIV biometrics are designed to support a cardholder-to-external system (CTE) authentication mechanism through a match-off-card scheme. The following subsections define two authentication schemes that make use of the PIV biometrics.[22]

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

[22] As noted in Section 4.2.3.1, neither the fingerprint templates nor the iris images are guaranteed to be present on a PIV Card, since it may not be possible to collect fingerprints from some cardholders and iris images collection is optional. When biometric authentication cannot be performed, PKI-AUTH is the recommended alternate authentication mechanism.

+ Slower mechanism, because it requires two interactions (e.g., presentation of PIN and biometric) with the cardholder.

+ Strong resistance to use of unaltered card by non-owner since PIN and cardholder biometric are required.

+ Digital signature on biometric, which is checked to further strengthen the mechanism.

+ Does not provide protection against use of a revoked card.

+ Applicable with contact card readers, and contactless card readers that support the virtual contact interface.

6.2.1.1 Unattended Authentication Using PIV Biometric (BIO)

The following steps shall be performed for unattended authentication of the PIV biometric:

+ The CHUID or another data element[23] is read from the card and is checked to ensure the card has not expired and that it is from a trusted source.

+ The cardholder is prompted to submit a PIN, activating the PIV Card.

+ The PIV biometric is read from the card.

+ The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. Note that the signature verification may require retrieval of the content signing certificate from the CHUID if the signature on the biometric was generated with the same key as the signature on the CHUID.

+ The cardholder is prompted to submit a live biometric sample.

+ If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card.

+ The FASC-N (or UUID) in the CHUID or other data element is compared with the FASC-N (or UUID) in the Signed Attributes field of the external digital signature on the biometric.

+ A unique identifier within the CHUID or other data element is used as input to the authorization check to determine whether the cardholder should be granted access.

6.2.1.2 Attended Authentication of PIV Biometric (BIO-A)

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

[23] The PIV Authentication certificate or Card Authentication certificate may be leveraged instead of the CHUID to verify that the card is not expired.

6.2.2 Authentication Using On-Card Biometric Comparison (OCC-AUTH)

The PIV Card Application may host the optional on-card biometric comparison algorithm. In this case, on-card biometric comparison data is stored on the card, which cannot be read, but could be used for identity verification. A live-scan biometric is supplied to the card to perform cardholder-to-card (CTC) authentication and the card responds with an indication of the success of the on-card biometric comparison. The response includes information that allows the reader to authenticate the card. The cardholder PIN is not required for this operation. The PIV Card shall include a mechanism to block this authentication mechanism after a number of consecutive failed authentication attempts as stipulated by the department or agency. As with authentication using the PIV biometrics, if agencies choose to implement on-card biometric comparison, it shall be implemented as defined in [SP 800-73] and [SP 800-76].

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

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

6.2.3 Authentication Using PIV Asymmetric Cryptography

The PIV Card contains two mandatory asymmetric authentication private keys and corresponding certificates to support cardholder-to-external system (CTE) authentication, as described in Section 4. The following subsections shall be used to perform authentication using the authentication keys.

6.2.3.1 Authentication with the PIV Authentication Certificate Credential (PKI-AUTH)

The following steps shall be performed for PKI-AUTH:

- The reader reads the PIV Authentication certificate from the PIV Card Application.
- The reader validates the PIV Authentication certificate from the PIV Card Application using standards-compliant PKI path validation[24] to ensure that it is neither expired nor revoked and that it is from a trusted source.
- The cardholder is prompted to submit a PIN, which is used to activate the card. (If implemented, other card activation mechanisms, as specified in [SP 800-73], may be used to activate the card.)
- The reader issues a challenge string to the card and requests an asymmetric operation in response.
- The card responds to the previously issued challenge by signing it using the PIV Authentication private key.
- The reader verifies that the card's response is the expected response to the issued challenge.

[24] Path validation should be configured to specify which policy OIDs are trusted. The policy OID for the PIV Authentication certificate is id-fpki-common-authentication.

- A unique identifier from the PIV Authentication certificate is extracted and passed as input to the access control decision.

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

- Requires the use of certificate status checking infrastructure.
- Highly resistant to credential forgery.
- Strong resistance to use of unaltered card by non-owner since card activation is required.
- Applicable with contact card readers, and contactless card readers that support the virtual contact interface.

6.2.3.2 Authentication with the Card Authentication Certificate Credential (PKI-CAK)

The following steps shall be performed for PKI-CAK:

- The reader reads the Card Authentication certificate from the PIV Card Application.
- The reader validates the Card Authentication certificate from the PIV Card Application using standards-compliant PKI path validation[25] to ensure that it is neither expired nor revoked and that it is from a trusted source.
- The reader issues a challenge string to the card and requests an asymmetric operation in response.
- The card responds to the previously issued challenge by signing it using the Card Authentication private key.
- The reader verifies that the card's response is the expected response to the issued challenge.
- A unique identifier from the Card Authentication certificate is extracted and passed as input to the access control decision.

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

- Requires the use of certificate status checking infrastructure.
- Highly resistant to credential forgery.
- Low resistance to use of unaltered card by non-owner of card.
- Applicable with contact and contactless readers.

[25] Path validation should be configured to specify which policy OIDs are trusted. The policy OID for the Card Authentication certificate is id-fpki-common-cardAuth.

6.2.4 Authentication with the Symmetric Card Authentication Key (SYM-CAK)

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

- The CHUID, PIV Authentication certificate, or Card Authentication certificate data element is read from the PIV Card and is checked to ensure the card has not expired.
- The digital signature on the data element is checked to ensure that it was signed by a trusted source and is unaltered.
- The reader issues a challenge string to the card and requests a response.
- The card responds to the previously issued challenge by encrypting the challenge using the symmetric Card Authentication key.
- The response is validated as the expected response to the issued challenge.
- A unique identifier within the data element is used as input to the authorization check to determine whether the cardholder should be granted access.

Some of the characteristics of the symmetric Card Authentication key authentication mechanism are as follows:

- Resistant to credential forgery.
- Does not provide protection against use of a revoked card.
- Low resistance to use of unaltered card by non-owner of card.
- Applicable with contact and contactless readers.

6.2.5 Authentication Using the CHUID

The PIV Card provides a mandatory logical credential called the CHUID. As described in Section 4.2.1, the CHUID contains numerous data elements.

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

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

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

- Can be used for rapid authentication for high volume access control.
- Low resistance to use of unaltered card by non-owner of card.
- Does not provide protection against use of a revoked card.
- Applicable with contact and contactless readers.

As the CHUID authentication mechanism provides LITTLE or NO assurance in the identity of the cardholder, use of the CHUID authentication mechanism is deprecated. It is expected that the CHUID authentication mechanism will be removed from this Standard at the next five-year revision.

6.2.6 Authentication Using PIV Visual Credentials (VIS)

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

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

- Zone 1F – Photograph;
- Zone 2F – Name;
- Zone 8F – Employee Affiliation;
- Zone 10F – Agency, Department, or Organization;
- Zones 14F and 19F – Card Expiration Date;
- Zone 15F – Color-Coding for Employee Affiliation;
- Zone 1B – Agency Card Serial Number (back of card);
- Zone 2B – Issuer Identification Number (back of card).

The PIV Card may also bear optional components, some of which are:

- Zone 11F – Agency Seal;
- Zone 5B – Physical Characteristics of Cardholder (back of card);
- Zone 3F – Signature.

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

- The guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way.

- The guard compares the cardholder's facial features with the picture on the card to ensure that they match.
- The guard checks the expiration date on the card to ensure that the card has not expired.
- The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional)
- The guard collects the cardholder's signature and compares it with the signature on the card. (Optional)
- One or more of the other data elements on the card (e.g., name, employee affiliation, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.

Some characteristics of the visual authentication mechanism are as follows:

- Human inspection of card, which is not amenable for rapid or high volume access control.
- Resistant to use of unaltered card by non-owner of card.
- Low resistance to tampering and forgery.
- Does not provide protection against use of a revoked card.
- Applicable in environments with and without 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 complementing authentication mechanisms may be applied in unison to achieve a higher degree of assurance of the identity of the PIV cardholder. For example, PKI-AUTH and BIO may be applied in unison to achieve a higher degree of assurance in cardholder identity.

Adequately designed and implemented relying systems can achieve the PIV Card authentication assurance levels stated in Tables 6-2 and 6-3. Less adequately designed or implemented relying systems may only achieve lower authentication assurance levels. The design of components of relying systems, including card readers, biometric readers, cryptographic modules, and key management systems, involves many factors not fully specified by FIPS 201, such as correctness of the functional mechanism, physical protection of the mechanism, and environmental conditions at the authentication point. Additional standards and best practice guidelines apply to the design and implementation of relying systems, e.g., [FIPS140] and [SP 800-116].

6.3.1 Physical Access

The PIV Card may be used to authenticate the identity of the cardholder in a physical access control environment. For example, a Federal facility may have physical entry doors that have human guards at checkpoints, or may have electronic access control points. The PIV-supported authentication mechanisms

for physical access control systems are summarized in Table 6-2. An authentication mechanism that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level. Moreover, the authentication mechanisms in Table 6-2 can be combined to achieve higher assurance levels.[26]

Table 6-2. Authentication for Physical Access

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

6.3.2 Logical Access

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

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

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
LITTLE or NO confidence	CHUID	
SOME confidence	PKI-CAK	PKI-CAK
HIGH confidence	BIO	
VERY HIGH confidence	BIO-A, OCC-AUTH, PKI-AUTH	PKI-AUTH

[26] Combinations of authentication mechanisms are specified in [SP 800-116].

Appendix A—PIV Validation, Certification, and Accreditation

This appendix provides compliance requirements for PIV validation, certification, and accreditation, and is normative.

A.1 Accreditation of PIV Card Issuers (PCI)

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

The four major accreditation topics identified in [SP 800-79] are:

- organizational preparedness;
- security management and data protection;
- infrastructure elements; and
- (PIV) processes.

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

- initiation phase;
- assessment phase;
- accreditation phase; and
- monitoring phase.

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

A.2 Application of Risk Management Framework to IT System(s) Supporting PCI

The accreditation of the capability and reliability of a PCI using the methodology outlined in [SP 800-79] depends upon adequate security for the information systems that are used for PCI functions. The assurance that such a security exists in a PCI is obtained through evidence of the application of the Risk Management Framework guidelines specified in [SP 800-37]. The methodology in [SP 800-37] in turn was created pursuant to a mandate in Appendix III of Office of Management and Budget (OMB) Circular A-130. An Information system authorization decision together with evidence of security control monitoring compliant with [SP 800-37] guidelines signifies that a PCI organization's official accepts responsibility for the security (in terms of confidentiality, integrity, and availability of information) of the information systems that will be involved in carrying out the PCI functions. Hence evidence of successful application of Risk Management Framework consistent with [SP 800-37] guidelines is mandatory for issuing PCI accreditation using SP 800-79.

A.3 Conformance Testing of PIV Card Application and Middleware

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

A.4 Cryptographic Testing and Validation

All on-card cryptographic modules hosting the PIV Card Application and cryptographic modules of card issuance and maintenance systems shall be validated to [FIPS140] with an overall Security Level 2 (or higher). The facilities for [FIPS140] testing are the Cryptographic and Security Testing laboratories accredited by the NVLAP program of NIST. Vendors wanting to supply cryptographic modules can select any of the accredited laboratories. The tests conducted by these laboratories for all vendor submissions are validated and a validation certificate for each vendor module is issued by the Cryptographic Module Validation Program (CMVP), a joint program run by NIST and the Communications Security Establishment (CSE) of the Government of Canada. The details of the CMVP and NVLAP programs and the list of testing laboratories can be found at the CMVP Web site at http://csrc.nist.gov/groups/STM/cmvp/index.html.

A.5 FIPS 201 Evaluation Program

In order to evaluate the conformance of different families of products that support the PIV processes to this Standard and its associated technical specifications, the Office of Governmentwide Policy under GSA set up the FIPS 201 Evaluation Program. The product families currently include card personalization products, card readers, products involved in credential enrollment functions such as fingerprint and facial image capture equipment, biometric fingerprint template generators, etc. Products evaluated and approved under this program are placed on the FIPS 201 Approved Products List to enable procurement of conformant products by implementing agencies. The details of the program are available at http://fips201ep.cio.gov/.

Appendix B—PIV Object Identifiers and Certificate Extension

This normative appendix provides additional details for the PIV objects identified in Section 4.

B.1 PIV Object Identifiers

Table B-1 lists details for PIV object identifiers.

Table B-1. PIV Object Identifiers

ID	Object Identifier	Description
PIV eContent Types		
id-PIV-CHUIDSecurityObject	2.16.840.1.101.3.6.1	The associated content is the concatenated contents of the CHUID, excluding the authentication key map[27] and the asymmetric signature field.
id-PIV-biometricObject	2.16.840.1.101.3.6.2	The associated content is the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD.
PIV Attributes		
pivCardholder-Name	2.16.840.1.101.3.6.3	The attribute value is of type DirectoryString and specifies the PIV cardholder's name.
pivCardholder-DN	2.16.840.1.101.3.6.4	The attribute value is an X.501 type Name and specifies the DN associated with the PIV cardholder in the PIV certificate(s).
pivSigner-DN	2.16.840.1.101.3.6.5	The attribute value is an X.501 type Name and specifies the subject name that appears in the PKI certificate for the entity that signed the biometric or CHUID.
pivFASC-N	2.16.840.1.101.3.6.6	The pivFASC-N OID may appear as a name type in the otherName field of the subjectAltName extension of X.509 certificates or a signed attribute in CMS external signatures. Where used as a name type, the syntax is OCTET STRING. Where used as an attribute, the attribute value is of type OCTET STRING. In each case, the value specifies the FASC-N of the PIV Card.
PIV Extended Key Usage		
id-PIV-content-signing	2.16.840.1.101.3.6.7	This specifies that the public key may be used to verify signatures on 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.

The OIDs for certificate policies are specified in [COMMON].

B.2 PIV Certificate Extension

The PIV NACI indicator (background investigation indicator) extension indicates whether the subject's background investigation was incomplete at the time of credential issuance. The PIV NACI indicator (background investigation indicator) extension is always non-critical, and shall appear in all PIV

[27] The authentication key map was deprecated in SP 800-73-2 and was removed from SP 800-73-3.

Authentication certificates and Card Authentication certificates. The value of this extension is asserted as follows:

- TRUE if, at the time of credential issuance, (1) the FBI National Criminal History Fingerprint Check has completed, and (2) a background investigation has been initiated but has not completed.
- FALSE if, at the time of credential issuance, the subject's background investigation has been completed and successfully adjudicated.

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

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

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NONE --

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

NACI-indicator ::= BOOLEAN

END
```

Appendix C—Glossary of Terms, Acronyms, and Notations

This informative appendix describes the vocabulary and textual representations used in the document.

C.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, a government affiliate, or a contractor.[28]

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.

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 iris image 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).

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

Cardholder: An individual possessing an issued PIV Card.

Card Management System: The card management system manages the lifecycle of a PIV Card Application.

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

[28] See Page 2 of [OMB0524] for further details of individuals who are eligible to be issued PIV Cards.

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

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

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

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, issuer, 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.

E-Authentication Assurance Level: A measure of trust or confidence in an authentication mechanism defined in [OMB0404] and [SP 800-63], in terms of four levels:

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

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

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

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.

Hash Function: A function that maps a bit string of arbitrary length to a fixed length bit string. Secure hash functions [FIPS180] 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 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 Proofing: The process of providing sufficient information (e.g., identity history, credentials, documents) 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.

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

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

Key: See "Cryptographic Key."

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

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

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.

On-Card Comparison: Comparison of fingerprint data transmitted to the card with reference data previously stored on the card.

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

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

Personally Identifiable Information (PII): Information that can be used to distinguish or trace an individual's identity, such as name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information that is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc. [OMB0716]

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

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

Private Key: The secret part of an asymmetric key pair that is typically used to digitally sign or decrypt data.

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

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

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

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

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

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.

Registration: See "Identity Registration."

Symmetric Key: A cryptographic key that is used to perform both the cryptographic operation and its inverse, for example to encrypt and decrypt, or create a message authentication code and to verify the code.

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."

C.2 Acronyms

The following acronyms and abbreviations are used throughout this Standard:

ACL	Access Control List
AES	Advanced Encryption Standard
AID	Application IDentifier
AIM	Association for Automatic Identification and Mobility
ANSI	American National Standards Institute
ARC	Automated Record Checks
ASTM	American Society for Testing and Materials
CA	Certification Authority
CAK	Card Authentication Key
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Cardholder Unique Identifier
cm	Centimeter
CMS	Cryptographic Message Syntax
CMTC	Card Management System to the Card
CMVP	Cryptographic Module Validation Program
COTS	Commercial Off-the-Shelf
CRL	Certificate Revocation List
CSE	Communications Security Establishment
CTC	Cardholder to Card
CTE	Cardholder to External System
DHS	Department of Homeland Security
DN	Distinguished Name
DOB	Date of Birth
dpi	Dots Per Inch
ERT	Emergency Response Team
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FBI	Federal Bureau of Investigation
FIPS	Federal Information Processing Standards
FIPS PUB	FIPS Publication
FISMA	Federal Information Security Management Act
GSA	U.S. General Services Administration
GUID	Global Unique Identification Number

HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
I&A	Identification and Authentication
IAB	Interagency Advisory Board
ICAMSC	Identity, Credential, and Access Management Subcommittee
ICC	Integrated Circuit Chip
ID	Identification
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INCITS	International Committee for Information Technology Standards
ISO	International Organization for Standardization
IT	Information Technology
ITL	Information Technology Laboratory
LDAP	Lightweight Directory Access Protocol
mm	Millimeter
MWR	Morale, Welfare, and Recreation
NAC	National Agency Check
NACI	National Agency Check with Written Inquiries
NCHC	National Criminal History Check
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
NPIVP	NIST Personal Identity Verification Program
NVLAP	National Voluntary Laboratory Accreditation Program
OCC	On-Card Biometric Comparison
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OMB	Office of Management and Budget
OPM	Office of Personnel Management
PCI	PIV Card Issuer
PC/SC	Personal Computer/Smart Card
PDF	Portable Data File
PIA	Privacy Impact Assessment
PII	Personally Identifiable Information
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
RFC	Request for Comments
SES	Senior Executive Service
SP	Special Publication
SSP	Shared Service Provider
TSA	Transportation Security Administration

URI	Uniform Resource Identifier
U.S.C.	United States Code
UUID	Universally Unique IDentifier

C.3 Notations

This Standard uses the following typographical conventions in text:

- ASN.1 data types are represented in *italics*. For example, *SignedData* and *SignerInfo* are data types defined for digital signatures.

- Letters or words in CAPITALS separated with underscore represent CBEFF-compliant data structures. For example, CBEFF_HEADER is a header field in the CBEFF structure.

Appendix D—References

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

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

[COMMON] *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, Version 3647 – 1.17, December 9, 2011, or as amended. Available at http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf.

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

[FIS] *Federal Investigative Standards*, OPM.

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

[FIPS180] FIPS Publication 180-4, *Secure Hash Standard (SHS)*, March 2012, or as amended. Available at http://csrc.nist.gov/publications/fips/fips180-4/fips-180-4.pdf.

[FISMA] *Federal Information Security Management Act of 2002*. Available at http://csrc.nist.gov/drivers/documents/FISMA-final.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.

[ISO3166] ISO 3166-1:2006. *Codes for the representation of names of countries and their subdivisions—Part 1: Country codes*.

[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.

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

[OMB0322] OMB Memorandum M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003.

[OMB0404] OMB Memorandum M-04-04, *E-Authentication Guidance for Federal Agencies*, OMB, December 2003.

[OMB0524] OMB Memorandum M-05-24, *Implementation of Homeland Security Presidential Directive (HSPD) 12 – Policy for a Common Identification Standard for Federal Employees and Contractors*, OMB, August 2005.

[OMB0618] OMB Memorandum M-06-18, *Acquisition of Products and Services for Implementation of HSPD-12*, June 2006.

[OMB0716] OMB Memorandum M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, OMB, May 2007.

[OMB1111] OMB Memorandum M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD) 12–Policy for a Common Identification Standard for Federal Employees and Contractors*, February 2011.

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

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

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

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

[RFC4122] RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*, Internet Engineering Task Force (IETF), July 2005. Available at http://www.ietf.org/rfc/rfc4122.txt.

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

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

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

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

[SP 800-59] NIST Special Publication 800-59, *Guideline for Identifying an Information System as a National Security System,* NIST, August 2003 or as amended.

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

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

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

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

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

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

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

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

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

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

[SP 800-156] NIST Special Publication 800-156, *Representation of PIV Chain-of-Trust for Import and Export,* NIST.

[SP 800-157] NIST Special Publication 800-157, *Guidelines for Personal Identity Verification (PIV) Derived Credentials,* NIST.

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

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

2310

2311 ## Appendix E—Revision History

2312 The Revision History provides an overview of the changes to FIPS 201 since its initial release.

Version	Release Date	Updates
FIPS 201	February 2005	Initial Release
FIPS 201-1	March 2006	Added the requirement for electronically distinguishable from identity credentials issued to individuals who have a completed investigation (NACI Indictor).
FIPS 201-1 Change Notice 1	March 2006	Added clarification for variable placement of Agency Card Serial Number along the outer edge of the back of the PIV Card is allowed. Also, updated ASN.1 encoding for NACI Indicator (background investigation indicator).
FIPS 201-2, Revised Draft	May 2012	This version represents the 5-year review of FIPS 201 and change request inputs received from agencies. Following are the highlights of changes made in this version. Modified the requirement for accreditation of PIV Card issuer to include an independent review. Incorporated references to credentialing guidance and requirements issued by OPM and OMB. Made the facial image data element on the PIV Card mandatory. Added the option to collect and store iris biometric data on the PIV Card. Added option to use electronic facial image for authentication in operator-attended environments. Incorporated the content from Form I-9 that is relevant to FIPS 201. Introduced the concept of a “chain-of-trust” optionally maintained by a PIV Card issuer. Changed the maximum life of PIV Card from 5 years to 6 years. Added requirements for issuing a PIV Card to an individual under a pseudonymous identity. Added requirements for issuing a PIV Card to an individual within grace period. Added requirements for post-issuance updates. Added option to allow for remote PIN resets. Introduced the ability to issue PIV derived credentials. The employee affiliation color-coding and the large expiration date in the upper right-hand corner of the card are now mandatory. Made all four asymmetric keys and certificates mandatory. Introduced the concept of a virtual contact interface over which all functionality of the PIV Card is accessible. Added a mandatory UUID as a unique identifier for the PIV

		Card in addition to the FASC-N. Added optional on-card biometric comparison as a means of performing card activation and as a PIV authentication mechanism. Removed direct requirement to distribute certificates and CRLs via LDAP. Updated authentication mechanisms to enable variations in implementations. Require signature verification and certification path validation in the CHUID, BIO, and BIO-A authentication mechanisms. The VIS and CHUID authentication mechanisms have been downgraded to indicate that they provide LITTLE or NO assurance in the identity of the cardholder. Deprecated the use of the CHUID authentication mechanism. The CHUID data element has not been deprecated and continues to be mandatory.

2313