



Federal Identity Management Handbook

PUBLIC DRAFT

March 2005

Acknowledgements

The Office of Management and Budget and the Federal Identity Credentialing Committee would like to acknowledge the significant contributions of the National Institute of Standards and Technology (NIST) and the Government Smart Card Interagency Advisory Board (IAB) for providing valuable contributions to the development of this handbook.

A special thanks goes out to those who participated in the various workshops and provided valuable subject matter expertise and lessons learned. The comments received from other government and industry organizations are also acknowledged.

Table of Contents

1. Introduction	1
1.1 Purpose	1
1.2 Federal Identity Credentialing Committee/Interagency Advisory Board.....	1
1.3 Business and Policy.....	2
1.3.1 Office of Management and Budget (OMB) Guidance	2
1.3.2 HSPD-12.....	3
1.3.3 HSPD 12 Agency Plan.....	5
1.3.4 HSPD 12 Agency Plan Frequently Asked Questions.....	5
1.3.5 HSPD-12 Implementation Roadmap.....	5
2. PIV I—Common Identification, Security, and Privacy Requirements	7
2.1 Control Objectives	7
2.2 Identity Proofing and Registration.....	8
2.2.1 Identity-Proofing Recommendations.....	10
2.2.2 Temporary Access and Access-Pending Authorization	10
2.2.3 Agency Affiliates and Agency Partners.....	10
2.2.4 Identity Source Documents.....	10
2.2.5 Notifications and Document Management	11
2.2.6 Background Checks.....	11
2.3 PIV I Card Issuance and Maintenance	12
2.3.1 General Requirements for PIV I Issuance and Maintenance	12
2.3.2 Role-Based Model Example	13
2.3.3 System-Based Model Example.....	20
2.3.4 Suspension, Revocation, and Destruction	24
2.3.5 Reissuance to Current PIV Cardholders.....	24
2.4 Privacy Requirements.....	25
2.4.1 Protecting Personal Privacy	25
2.4.2 Agency Requirements.....	25
2.5 PIV Card Lifecycle	29
2.5.1 Managing the PIV Card Lifecycle.....	29
2.5.2 Suggested Card Lifecycle Management Methodology.....	30
2.5.3 Card Lifecycle Management Implementation.....	31
3. PIV - Validation, Certification, and Accreditation	35
3.1 FIPS 201 Requirements.....	35
3.2 NIST SP 800-37.....	36
3.3 Summary	37
4. PIV II - Front-End Subsystem	38
4.1 Physical PIV Card Requirements.....	38
4.1.1 Physical PIV Card Topology	38
4.1.2 Implementation Recommendations	54

Federal Identity Management Handbook

4.1.3	PIV Logical Data	57
4.1.4	Communication with the User Community	59
4.2	Logical Access Control	59
4.2.1	PIV Card Cryptographic Specifications	59
4.2.2	Cryptographic Implementation Guidance.....	60
4.3	Physical Access Control	61
4.3.1	Physical Access Control System Components	62
4.3.2	Physical Access Interoperability Guidelines.....	63
4.4	Biometric Data Specifications	66
4.4.1	Use of Biometric Technologies	66
4.4.2	Biometric Data Requirements.....	66
4.4.3	Biometric Technology Implementation Guidance.....	67
4.5	Card Reader Specifications	71
4.5.1	Smart Card Readers	71
4.5.2	Card Reader Compliance Requirements	72
4.5.3	Card Reader Implementation Guidance.....	72
4.6	PIV II – Identity Proofing, Registration, Issuance and Management	74
4.6.1	PIV II Identity Proofing and Registration Requirements	74
4.6.2	PIV II Card Issuance Requirements.....	75
4.6.3	PIV Card Maintenance.....	77
4.6.4	Key Management.....	81
4.7	Card Authentication	86
4.7.1	Identity Authentication Assurance Levels	86
4.7.2	Card Authentication Mechanisms	88
4.7.3	Graduated Identity Assurance Levels	92
4.8	PIV II – Special Technical Publication 800-73	93
5.	Implementation Planning.....	94
5.1	Acquisition Planning	94
5.1.1	Funding Streams	95
5.1.2	Current Methods of Procurement.....	96
5.1.3	Major Components of an Identity-Management System	97
5.1.4	Anticipating Implementation Costs.....	98
5.1.5	Agency PIV Sponsorship	101
5.1.6	Shared Service Provider.....	101
5.1.7	Acquisition Planning Template.....	104
5.2	Migration Planning	105
5.2.1	HSPD-12 Guidance	105
5.2.2	OMB Implementation Guidance.....	105
5.2.3	Key Benefits of Business and Systems Integration.....	105
5.2.4	Developing the Migration Plan	106
5.3	Lessons Learned	111
5.3.1	Implementation Management	111
5.3.2	Stakeholder Management.....	112
5.3.3	Procurement Plan	112

Federal Identity Management Handbook

5.3.4	System Design.....	113
5.3.5	System Interoperability	113
5.3.6	Pilot and Production.....	113
5.3.7	Post-Operational Processes	114
5.3.8	Training.....	114
5.4	Case Studies	114
5.4.1	U.S. Department of State.....	117
5.4.2	U.S. Department of Interior	118
5.4.3	U.S. Department of Homeland Security	119
5.5	Conformance Testing.....	120
5.5.1	Why Conformance Testing is Needed	120
5.5.2	How Conformance Testing is Performed	120
5.6	Reference Implementation.....	123
6.	APPENDIX A – Sample Acquisition Planning Template.....	125
7.	APPENDIX B – Implementation Checklist	131
8.	APPENDIX C – Sample PIV Request Form.....	145
9.	APPENDIX D – GSA Technical Supplement to OMB M-05-05.....	146
10.	INDEX	149

List of Figures

Figure 1. Sample Card Lifecycle Methodology	30
Figure 2. Certification and Accreditation Methodology Overview.....	37
Figure 3. PIV Card Front – Printable Areas and Required Data	42
Figure 4. Card Back – Printable Areas and Required Data	44
Figure 5. Card Front – Optional Data Placement – Example 1	47
Figure 6. Card Front – Optional Data Placement – Example 2.....	48
Figure 7. Card Front – Optional Data Placement – Example 3.....	49
Figure 8. Card Front – Optional Data Placement – Example 4.....	50
Figure 9. Card Back – Optional Data Placement – Example 1	52
Figure 10. Card Back – Optional Data Placement – Example 2	53
Figure 11. Physical Access Control System	63
Figure 12. Fingerprint Enrollment and Authentication Process Flow	68
Figure 13. Balancing Card Reader Assurance Levels with Convenience.....	74
Figure 14. PIV Identity Verification and Issuance	75
Figure 15. Example Organization Structure for Agencies PIV Implementation.....	95
Figure 16. Identity Management Components and Examples of the Assets Required..	98
Figure 17. Four Primary Components of SSP Certification and Accreditation Process	103
Figure 18. Identity Management Convergence Architecture.....	106
Figure 19. FIPS 201 Migration Plan Roadmap	108
Figure 20. FIPS 201 Card and Middleware Test Process.....	121
Figure 21. NIST Reference Implementation Architecture	123

List of Tables

Table 1. PIV System Components and Validation Requirements 36

Table 2. PIV Card Topology Elements (Card Front) 39

Table 3. PIV Card Topology Elements (Card Back)..... 40

Table 4. PIV Card Mandatory Logical Elements and Categories of Use 57

Table 5. Optional Logical Elements and Categories of Use..... 58

Table 6. PIV Key Types 61

Table 7. FIPS 201 Biometric Data Requirements 66

Table 8. Mandated CRL Publication Frequencies..... 84

Table 9. Scenarios Affecting CA Performance and Recommended Responses 86

Table 10. OMB E-Authentication and PIV Assurance Levels 87

Table 11. Advantages and Disadvantages of Authentication Methods..... 89

Table 12. Assurance Levels and Authentication Mechanisms for Physical and Logical Access..... 93

Table 13. Potential FIPS 201 Acquisition Stakeholders..... 96

Table 14. Amount of Time Required to Train PIV Roles 96

Table 15. Sample Smart-Card Related Products List 100

Table 16. Ongoing Federal Smart Card Technology Initiatives by Department..... 115

Table 17. Integrated Federal Smart Card Implementations by Agency 116

1. Introduction

1.1 Purpose

E-Government, an integral part of the President's Management Agenda (PMA), is defined as the use of digital technologies to transform government operations in order to improve effectiveness, efficiency, and service delivery. As the Federal Government modernizes internal processes and adopts cross-agency applications available to all Federal employees, a common, trusted basis for authenticating the identity of individuals within the Federal sector is required. Additionally, in accordance with the President's vision of creating a more responsive and cost-effective government, the Office of Management and Budget (OMB), provided a memo to Federal Chief Information Officers (CIOs), outlining details of the E-Government initiative on authentication and identity management OMB Memorandum dated 3 July 2003, Subject: Streamlining Authentication and Identity Management within the Federal Government (<http://www.whitehouse.gov/omb/inforeg/eauth.pdf>). The OMB memo also charged the Federal Identity Credentialing Committee (FICC) to develop a "Common comprehensive policy for credentialing of Federal employees."

On August 27, 2004, a Homeland Security Presidential Directive was issued entitled HSPD-12, "Policy for a Common Identification Standard for Federal Employees and Contractors." HSPD-12 directed the promulgation of a new Federal standard for secure and reliable identification issued by Federal agencies for their employees and contractors. In response to the directive, the National Institute of Standards and Technology (NIST) published Federal Information Processing Standards Publication 201 (FIPS 201) on February 25, 2005. FIPS 201 and its associated Special Publications provide a detailed specification for Federal agencies and departments deploying a personal identity verification (PIV) card for their employees and contractors. The FIPS 201 standard can be accessed from the NIST web site at <http://csrc.nist.gov/piv-project/index.html>.

Once implemented, a secure and interoperable Personal Identity Verification (PIV) card will provide the attributes of security, authentication, identity verification, trust, and privacy to a commonly accepted identification card for Federal employees and contractors. Privileges granted to the PIV cardholder will remain a local agency decision. The PIV card is a core component to setting the "trust model" across the Federal enterprise.

1.2 Federal Identity Credentialing Committee/Interagency Advisory Board

The FICC is composed of representatives from the major Federal agencies and departments. Its purpose is to make policy recommendations and develop the Federal Identity Credentialing Component of the Federal Enterprise Architecture. This includes associated services including identity proofing and identity credential management for the Federal government. Members of the FICC also champion these activities at the agencies they represent.

The Smart Card Interagency Advisory Board (IAB) works with the FICC and is composed of representatives from the major Federal agencies and departments skilled in implementing physical access control systems with smart-card related technology. The IAB conducts analyses and provides

Federal Identity Management Handbook

recommendations to government and industry on technology issues related to the efficient use of smart cards and related products for use by components of the United States Government.

This handbook was developed in collaboration with the FICC, IAB, and OMB. It is offered as guidance for government agency credentialing managers, their leadership, and other stakeholders as they pursue compliance with HSPD 12 and FIPS 201. The handbook provides specific implementation direction on course of action, schedule requirements, acquisition planning, migration planning, lessons learned, and case studies.

For the Federal government to fully realize the benefits of electronic government, a ubiquitous and consistent method of providing identity credentials is necessary for both electronic security (logical access) and building security (physical access) within the Federal sector. As the Federal government modernizes internal processes to reduce costs for agency administration and moves to cross-agency applications that are available to all Federal employees, a common, trusted basis is needed for authentication. FIPS 201 provides for the issuance of PIV cards for Federal employees and contractors that provide sufficient identity assurance to satisfy a variety of government-wide application and access control requirements.

1.3 Business and Policy

The management of identity credentialing policy is administered by the FICC with input received from FICC working groups, the IAB, the Federal PKI Policy Authority, OMB, and other Federal agencies. The goal is to establish a comprehensive set of policies that allow for robust, efficient and interoperable identity credentialing systems across the Federal enterprise. Policy that relates to privilege granting and building access control will continue to be managed by individual agencies. To maintain a common understanding of the latest developments in Federal credentialing, agencies are encouraged to follow the developments of the FICC (see www.cio.gov/ficc), the Smart Card Project Managers group, and the Smart Card IAB (see www.smart.gov).

The FICC makes recommendations regarding establishment, demonstration, and operation of a Federal Identity Credentialing component to the CIO Council and the OMB. It also provides a focal point for the implementation of the component, including support of migration to a shared service concept endorsed as part of the Federal Enterprise Architecture. Policy recommendations and guidance provided by the FICC identify and resolve Federal identity credentialing technical and business issues and recommend solutions to policy and interoperability issues.

1.3.1 Office of Management and Budget (OMB) Guidance

Placeholder

1.3.2 HSPD-12



For Immediate Release
Office of the Press Secretary
August 27, 2004

Homeland Security Presidential Directive/Hspd-12

Subject: Policy for a Common Identification Standard for Federal Employees and Contractors

(1) Wide variations in the quality and security of forms of identification used to gain access to secure Federal and other facilities where there is potential for terrorist attacks need to be eliminated. Therefore, it is the policy of the United States to enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy by establishing a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors (including contractor employees).

(2) To implement the policy set forth in paragraph (1), the Secretary of Commerce shall promulgate in accordance with applicable law a Federal standard for secure and reliable forms of identification (the "Standard") not later than 6 months after the date of this directive in consultation with the Secretary of State, the Secretary of Defense, the Attorney General, the Secretary of Homeland Security, the Director of the Office of Management and Budget (OMB), and the Director of the Office of Science and Technology Policy. The Secretary of Commerce shall periodically review the Standard and update the Standard as appropriate in consultation with the affected agencies.

(3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. The Standard will include graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application. The Standard shall not apply to identification associated with national security systems as defined by 44 U.S.C. 3542(b)(2).

(4) Not later than 4 months following promulgation of the Standard, the heads of executive departments and agencies shall have a program in place to ensure that identification issued by their departments and agencies to Federal employees and contractors meets the Standard. As promptly as possible, but in no case later than 8 months after the date of promulgation of the Standard, the heads of executive departments and agencies shall, to the maximum extent practicable, require the use of identification by Federal employees and contractors that meets the Standard in gaining physical access to Federally controlled facilities and logical access to Federally controlled information systems. Departments and agencies shall implement this directive in a manner consistent with ongoing Government-wide activities, policies and guidance issued by OMB, which shall ensure compliance.

Federal Identity Management Handbook

(5) Not later than 6 months following promulgation of the Standard, the heads of executive departments and agencies shall identify to the Assistant to the President for Homeland Security and the Director of OMB those Federally controlled facilities, Federally controlled information systems, and other Federal applications that are important for security and for which use of the Standard in circumstances not covered by this directive should be considered. Not later than 7 months following the promulgation of the Standard, the Assistant to the President for Homeland Security and the Director of OMB shall make recommendations to the President concerning possible use of the Standard for such additional Federal applications.

(6) This directive shall be implemented in a manner consistent with the Constitution and applicable laws, including the Privacy Act (5 U.S.C. 552a) and other statutes protecting the rights of Americans.

(7) Nothing in this directive alters, or impedes the ability to carry out, the authorities of the Federal departments and agencies to perform their responsibilities under law and consistent with applicable legal authorities and presidential guidance. This directive is intended only to improve the internal management of the executive branch of the Federal Government, and it is not intended to, and does not, create any right or benefit enforceable at law or in equity by any party against the United States, its departments, agencies, entities, officers, employees or agents, or any other person.

(8) The Assistant to the President for Homeland Security shall report to me not later than 7 months after the promulgation of the Standard on progress made to implement this directive, and shall thereafter report to me on such progress or any recommended changes from time to time as appropriate.

GEORGE W. BUSH

###

1.3.3 HSPD 12 Agency Plan

Placeholder

1.3.4 HSPD 12 Agency Plan Frequently Asked Questions

Placeholder

1.3.5 HSPD-12 Implementation Roadmap

Since every Government agency and/or department is conceivably at different points in the deployment of their current employee identification programs, it would be difficult to establish an approach to HSPD-12 implementation that would fit every situation. Recognizing this, in an effort to assist the reader, this section will present a high level roadmap as a guide to making the best use of this handbook.

The handbook is structured similarly to the NIST FIPS PUB 201 document and is divided into two major parts: PIV I and PIV II. PIV I addresses methods for complying with the requirements for common identification, security and privacy. PIV II addresses methods for complying with the technology and migration requirements for a secure and interoperable PIV. The handbook presents guidance in other areas as well. For example, Section 1.3 contains a template, called the HSPD-12 Agency Plan, to assist agencies in their response to OMB regarding the status of their HSPD-12 plans. Section 5 contains useful information on acquisition planning, migration planning, lessons learned and presents examples of case studies of existing successful agency implementations. Section 5 also includes information on the development of a FIPS 201 product conformance test suite, and a FIPS 201 baseline reference implementation which is currently under development with a planned completion in mid 2005.

The reader can read the handbook from cover to cover or a specific section at a time. Agency implementers might want to use the Table of Contents or the Index to find a topic they wish to focus on and go to it directly. For example, the reader might want to start by gaining a better understanding of the near term requirements of PIV I. This can be accessed in Section 2. Following this, the reader may want to gain a better understanding of how to analyze their agency's current ID card environment to determine where they are relative to the goal. A method for performing this analysis is presented in Section 5.2, Migration Planning. Finally, a checklist is presented in Appendix B whose purpose is to enable implementers to track each step or requirement completed.

Although ostensibly at different starting points in their journey, agency implementers may wish to see an example outline of general steps that may be taken in meeting their HSPD-12 goals. An initial outline follows.

1. Gain a clear understanding of HSPD-12 and FIPS 201 requirements by reviewing NIST FIPS 201 PUB and supporting documents as well as Sections 2 and 4 of this handbook.
2. Review OMB's guidance and schedule for HSPD-12 compliance in Section 1.3 of this handbook.

Federal Identity Management Handbook

3. Review requirements for completing the HSPD-12 Agency Plan in Section 1.3 of this handbook.
4. Gain a clear understanding of your agency's current policies for Physical Access Control, Logical Access Control, Graduated Security Criteria and Information Privacy.
5. Involve the primary Agency Stakeholders in the process. (For starters usually Management, Security Chief, Information Technology, Human Resources) It's best to have regular sustained involvement from stakeholders rather than on an occasional basis. Section 5.2 of this handbook.
6. Reach agreement on future policy as it pertains to item 4 above. This is a key item because these policies will drive other decisions later.
7. Establish a list of objectives your agency wants to achieve while meeting the directive.
8. Using the policy decisions from item 6 above, develop an initial list of requirements for the project and an initial roadmap to achieve the objectives list in item 7.
9. When practicable, begin to analyze the budget requirements and funding sources outlined in Acquisition Planning, Section 5.1 of this handbook.
10. Compare the compliance requirements necessary to meet PIV I to your agency's current identity proofing, registration, issuance and maintenance process. Identify any gaps and add these to the plan. Remember that your agency's plan should ensure that the FIPS 201 requirements for privacy are implemented before PIV IDs are issued. Refer to Section 2.4.

Once the plan takes shape, continue to build on other aspects, keeping the plan as simple as possible. Research other successful implementations and learn from the experience of others. Depending on the size and scale of your agency or department, analyze and consider the possibility of utilizing Agency PIV Sponsorship, found in Section 5.1 of this handbook. We hope that this example provides assistance in developing the thought process for the formation of your agency's plan. As they proceed, agency implementers are encouraged to seek assistance from other subject matter experts such as GSA's Smart Card Project Office and qualified industry service providers, Section 5.1 of this handbook.

2. PIV I—Common Identification, Security, and Privacy Requirements

2.1 Control Objectives

HSPD-12 establishes control objectives for secure and reliable forms of identification. Federal departments and agencies shall implement government-wide identity proofing, registration, and issuance functions that accomplish the following:¹

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

HSPD-12 requires the implementation of the control objectives to protect the privacy of PIV subscribers.

Agencies are required to comply with the identity-proofing, registration, issuance, and maintenance processes to meet these control objectives no later than October 2005. To conform to these control objectives agencies should ensure that:²

- Credentials are only issued (1) to individuals under their true identity and (2) after a proper authority has authorized issuance of the credential.
- Only an individual with a completed background investigation on record is issued a credential.
- An individual is issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or state government picture ID.
- Fraudulent or altered identity source documents are not accepted as genuine.
- 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, 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 cannot issue a credential with an incorrect identity or to a person not entitled to the credential.

¹ FIPS PUB 201, *Federal Information Processing Standards Publication, Personal Identity Verification (PIV) for Federal Employees and Contractors*, February, 25 2005.

² Ibid.

Federal Identity Management Handbook

- An issued credential is not modified, duplicated, or forged.

The following sections of this handbook, in addition to FIPS 201, provide agencies with best practices, lessons learned, and case studies in identity management to assist agencies in complying with PIV I.

2.2 Identity Proofing and Registration

The FIPS 201 identity-proofing process constitutes a standard policy for Federal agencies to follow when they provide official Government identification for new employees and contractors. When the policy is followed consistently, it will help ensure that cardholders are who they claim to be. Adherence to a uniform identity-proofing process across the Federal Government will also help establish a level of trust among agencies. HSPD-12 and FIPS 201 require Federal agencies to comply with the standard for identity-proofing employees and contractors by October 2005.

Each Federal agency is responsible for verifying or validating the identity of individuals to whom it issues credentials. FIPS 201 establishes a specific level of trust in an individual's identity as part of a process that binds the ID card to an individual (e.g., employee or contractor). Once that level of trust is established, it is possible to establish a chain of trust among Government agencies. Establishing and binding a validated identity to a PIV credential at the time the credential is issued is the foundation for a trusted common identity credential accepted throughout the Federal enterprise.

FIPS 201 is composed of two major sections, PIV I and II. Both of these sections define requirements for the identity-proofing and registration process. The initial requirement for agencies is to comply with PIV I by October 2005. In order to be in compliance with PIV I, agencies should implement a certified and accredited identity-proofing, registration, and issuance process for PIV cards across their enterprise. Note that compliance with PIV I does not require the issuance of a PIV II compliant card.

Agency compliance with the PIV II component of the standard will occur at a date to be announced later. PIV II compliance will require that all new PIV cards conform to the technical and interoperability specifications for smart cards and related products found in SP800-73 and SP800-76.

Verifying an individual's identity is the first step. FIPS 201 mandates processes and provides guidance on both the source documents required to validate an individual's identity and the process for issuing a Federal ID card. This section of the handbook provides additional guidance to help agencies comply with these requirements.

A secure and robust identity-proofing process is the foundation for FIPS 201 compliance. A successful implementation of FIPS 201 is not contingent on technologies and systems only. If a PIV credential is issued based on a faulty identity-proofing process, the credential is compromised, no matter what technology it implements.

FIPS 201 specifies an identity verification chain of trust for Federal agencies. An identity verification chain of trust comprises a common set of identity vetting rules that are used by multiple entities so that they can accept and trust one another's credentials. The chain of trust assures all parties involved that each participating entity followed the vetting procedures to securely and accurately verify an individual's identity. One of the goals is to permit agencies other than the issuing agency to accept a credential and avoid the requirement to issue a separate credential. This goal is also reflected in the Control Objectives of HSPD-12.

Federal Identity Management Handbook

The identity-proofing and registration process defined in Section 2.2 of FIPS 201 applies to the following categories of employees:

- New employees, contractors and affiliates
- Current employees
- Foreign Service Nationals

A single identity-proofing and registration process is defined in FIPS 201 for government employees and contractors. With one exception, background checks are not required for current employees where the results of their most recent background check are on file and can be verified by the PIV official. This process also applies to foreign workers who are working for the Federal Government overseas (e.g., an Iraqi citizen working for the U.S. Agency for International Development); however, a process for registration and approval must be approved by the U.S. Department of State, Bureau of Diplomatic Security; except for foreign workers from other countries who are under the command of a U.S. area military commander. The procedures for these individuals vary by country.

General Requirements for PIV I Identity Proofing and Registration

Requirements for PIV I Identity Proofing and Registration are as follows:

1. Agencies must use an approved identity proofing and registration process.
2. The process must begin with the initiation of a National Agency Check with Inquiries (NACI) or another Office of Personnel Management (OPM) or National Security investigation required for Federal employment. For current employees, this requirement may be satisfied if the employee has a completed and successfully adjudicated NACI on file.
3. Before PIV credential issuance occurs, the National Agency Check (NAC) should be completed and properly adjudicated.
4. The applicant must appear at least once in person in front of a PIV official before credential issuance can take place.
5. During identity proofing, the applicant must provide two identity source documents in original form. The documents must be on the list of acceptable documents included in *I-9, OMB No. 1115-0136, Employment Eligibility*. One of the documents must be a valid (not expired) picture ID issued by a state government or the Federal Government.
6. The PIV identity-proofing, registration, and issuance process must adhere to the principle of separation of roles. No single individual should have the power to issue a PIV credential without the cooperation of another authorized person.

The department or agency Inspector General must accredit the agency's identity proofing and registration process, and the process must be approved in writing by the head of the department or agency. When approving the process in writing, departments or agencies should identify those individuals who have direct oversight responsibilities and accountability for the identity proofing and registration process.

2.2.1 Identity-Proofing Recommendations

2.2.2 Temporary Access and Access-Pending Authorization

No new employee or contractor can be issued a Federal identity card until the identity-proofing process, including the NAC, is completed and successfully adjudicated. A NAC can generally be completed within 2-4 weeks. Employees may require access to buildings and systems, pending the completion of their NAC. Also, certain individuals do not require a PIV card but do need access to facilities, such as individuals who fill vending machines. Individual agency procedures for temporary visitor access should be applied in both of these situations.

Although it is the responsibility of each agency to design its temporary badges, as a best practice it is recommended that agencies design temporary and visitor badges that are unique and not similar to an official PIV card. This practice eliminates the possibility of mistaking temporary and visitor badges for valid PIV credentials. The exact specifications of a PIV-compliant identity credential can be found in Section 4.1 of this document.

2.2.3 Agency Affiliates and Agency Partners

Many agencies have affiliates or partners that require logical and/or physical access to do their jobs and that do not fall under the category of employee or contractor. Examples of affiliates and partners are visiting professors, guest faculty or fellowship recipients, interns or temporary help, and task-force members. Each agency must determine whether these individuals require a PIV card. If so, then all identity-proofing and issuance requirements in FIPS 201 must be met. If agencies determine that affiliates and/or partners do not require a PIV card, agencies are encouraged to implement agency-specific visitor policies for these individuals. Agencies should be careful not to develop policies that overlap or contradict the FIPS 201 processes for identity proofing and issuance.

2.2.4 Identity Source Documents

Applicants are required to provide two forms of identification when applying for a PIV card. The following link provides the acceptable forms of identification listed *I-9, OMB No. 1115-0136, Employment Eligibility* (<http://uscis.gov/graphics/formsfee/forms/files/i-9.pdf>). Individuals involved in the PIV –identity-proofing process should be trained in document inspection. Additionally, individuals who are responsible for identity proofing within agencies need access to electronic (when available) and non-electronic means for verifying the authenticity of identity source documents.

The validity of identity source documents should be verified by electronic means whenever possible. Electronic methods that perform document verification are available commercially and most operate in a similar manner. An electronic reader reads the document, such as a driver's license. The reader confirms the likelihood that the document is valid. This check however, is not indicative of the trustworthiness of an individual. The electronic check only indicates that a document is not expired, forged, or altered.

The issuer of the identity source documents may also be able to provide a means to verify the document's authenticity electronically. If not, other methods are available. For example, manuals are available that list all valid state driver's licenses and their features and topology.

2.2.5 Notifications and Document Management

Agencies should develop a secure and robust workflow for notification when each step of the identity-proofing process for an applicant is completed (for example, notification that a credential can be issued). The workflow method that is implemented should:

- Be secure
- Be auditable
- Protect the applicant's privacy

Depending upon the volume of applicants, it may be beneficial for some agencies to implement a secure electronic workflow method for managing PIV notifications and documents.

Additionally, each agency requires proper security controls to manage the submission and storage of relevant identity source documents throughout the identity-proofing process. When identity source documents are transferred, either manually or electronically, it must be done securely. Some examples of secure transmissions include sending the documents using encrypted e-mail, exchanging the documents via secure intranet or internet connection, or placing the documents in a sealed and secure envelope and transporting them so that they are never out of the possession of the transporter. The United States Postal Service and several commercial companies provide secure transport of documents.

Additionally, it is the responsibility of the PIV Registrar (described in Section 2.3.2) and the IDMS (described in Section 2.3.3.2) to maintain the following documentation:

- Completed and signed PIV request
- Completed and signed SF 85 (or equivalent)
- Information related to the Applicant's identity source documents
- Results of the Applicant's background check
- Copies of the photograph and fingerprints of the Applicant
- Any additional documents used to prove the identity of the Applicant

The PIV Registrar and the IDMS should, at a minimum, maintain these documents for the life cycle of the Applicant's employment. Individual agencies may provide additional guidance concerning how long employees' identity source documents have to be maintained. The items that are maintained by the PIV Registrar and IDMS should be maintained securely. If the documents are maintained as hard copy, they should be stored in a secure facility. If the documents are maintained electronically, they should be stored in a secure database. Individual agencies should develop a standardized business process for storing and maintaining this information.

2.2.6 Background Checks

Background checks in the form of a NACI/NAC are required for all employees and contractors who apply for a PIV card. At a minimum, before a PIV card can be issued, a completed and adjudicated NAC has to be completed. The results of the NACI/NAC should be kept either electronically or in physical form while the individual is employed. Agencies should store the NACI/NAC in a secure location (logical or physical).

Federal Identity Management Handbook

The Federal Investigative Services arm of the OPM conducts all NAC/NACI checks for non-Department of Defense (DoD) employees. The Defense Security Services Agency conducts NAC/NACI checks for DoD employees. Standard NACs are composed of a Security/Suitability Investigations Index (SII), Defense Clearance and Investigation Index (DCII), FBI Name Check, and FBI National Criminal History Fingerprint Check.

A NACI is the basic and minimum investigation required for all new Federal employees. It consists of a NAC with written inquiries and search of records covering specific areas of an individual's background during the past 5 years (inquiries sent to current and past employers, schools attended, references, and local law enforcement authorities).³

Each agency will have differing requirements for determining if a NACI is satisfactory and thus credential issuance can take place. This is because NACIs do not present information in a pass or fail manner; they provide a report to agencies and then agencies can adjudicate the NACI and determine whether an individual should be issued a credential. For example a NACI may indicate that an individual has a poor credit rating. This may not always indicate that an individual won't be issued a PIV credential; individual agencies will have to make that determination. An example NACI and NAC can be found at the following location, <http://www.opm.gov/extra/investigate/IS-15.pdf>.

2.3 PIV I Card Issuance and Maintenance

Compliance with PIV I requires that all Federal identity cards be issued by a certified and accredited issuance process. Today, many Federal agencies are in different stages of development with regard to their credentialing strategies for physical and logical access. Some agencies are deploying chip-based smart card technology while others are not. Some agencies are deploying PKI credentials while others are not. Regardless of the type and form of identification an agency is issuing, all agencies must comply with PIV I card issuance control and security requirements by October 2005. This means that by October 2005, an agency may continue to issue its current employee identification; however, the controls and procedures surrounding the issuance of official government identification must be in compliance with PIV I. OMB will provide additional guidance on when interoperable PIV credentials must be issued that comply with PIV II card specifications.

2.3.1 General Requirements for PIV I Issuance and Maintenance

To achieve compliance with PIV I card issuance requirements, at a minimum the following must be met.

1. Agencies must use an approved, certified and documented credential issuance and maintenance process.
2. The PIV issuance process must ensure the completion and successful adjudication of a National Agency Check with Written Inquiries (NACI) or other OPM or National Security community investigation required for Federal employment
3. The credential must be revoked or withheld if the results of the NACI are deemed to be non-satisfactory by the issuing agency.

³ Ibid.

Federal Identity Management Handbook

4. Prior to the release of a PIV credential to an applicant, the issuer must complete the chain of trust by verifying that the photograph in the registration or enrollment record matches the applicant. Upon successful match, the issuer shall release the PIV credential to the applicant.
5. The NAC must be completed and adjudicated before issuance can take place.
6. Agencies must issue credentials through systems and providers whose reliability has been established by the agency and documented and approved in writing.

As with the identity proofing and registration process, by October 2005 the department or agency Inspector General must accredit the PIV issuance and maintenance process adopted for that particular agency and the head of the department or agency must approve the process in writing.

As a requirement of the FIPS 201, by October 2005, Federal agencies must document their PIV issuance and maintenance policy, validate the reliability of the systems and providers that issue credentials, and approve their reliability in writing. This is one of the control objectives stated in HSPD-12. Fundamentally, reliability of the systems and providers who issue credentials should indicate that those systems and providers are accredited and secure. NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*,⁴ should be used by agencies to validate reliability.

There are currently two models for identity proofing, registration, issuance, and maintenance of Federal credentials that meet the control objectives for PIV I. They are the role-based model and system-based model. These models are provided as examples below. Agencies are permitted to implement their own model as long as requirements 1-6 listed above are met.

2.3.2 Role-Based Model Example

The role-based model assigns PIV identity-proofing responsibilities to individuals, based on the roles and functions they perform. In this model, one person cannot perform multiple roles; with one exception: the PIV Issuer and PIV Digital Signatory functions may be performed by the same entity. This requirement safeguards against the possibility of collusion between an applicant and one of the other roles.

Individual agencies will determine who performs each role for that agency. Each agency should also implement training for the roles. Training requirements for identity-proofing roles are detailed below.

2.3.2.1 Description of Roles

The PIV role based identity proofing process defines the following roles:

- Applicant
- PIV Sponsor
- PIV Registrar
- PIV Issuer

⁴ NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*, NIST, May 2004.

Federal Identity Management Handbook

- PIV Digital Signatory
- PIV Authentication Certification Authority (CA)

The **Applicant** is the individual to whom a PIV card will be issued once the PIV Registrar approves the application and the appropriate background checks have taken place.

In support of the application process, the Applicant should complete the following activities:

- Complete an SF 85 or equivalent.
- Present two forms of identification included in the acceptable documents list included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. One of the identification forms must be a valid state or Federal issued picture ID.
- Successfully complete the Applicant training modules.

The **PIV Sponsor** is the individual who validates an Applicant's requirement for a PIV credential and sponsors the Applicant's request.

The PIV Sponsor should meet the following minimum standards:

- Be a government official and be authorized in writing by the agency to request a PIV card
- Have valid justification for requesting a PIV card for an Applicant
- Be in a position of responsibility for the agency
- Have already been issued a valid PIV card
- Have successfully completed the Federal PIV Sponsor training modules

The **PIV Registrar** is the individual or entity that performs the identity-proofing process for the Applicant and ensures that the proper background checks have taken place with positive results. The PIV Registrar has final approval authority for issuance of a PIV credential to an Applicant. Once the background check is completed successfully, the PIV Registrar notifies the PIV Issuer that a PIV credential can be issued to the Applicant and that no other background checks are required.

The PIV Registrar should meet the following minimum standards:

- Be a government official and be designated in writing as a PIV Registrar.
- Be able to assess the reasonableness of the Applicant's identity-proofing documents. Reasonableness in this context indicates that the PIV Registrar is trained to detect any improprieties in the Applicant's identity-proofing documents.
- Be able to evaluate whether a PIV application is satisfactory and apply agency-specific processes to an unsatisfactory PIV application. Thus, the PIV Registrar needs training on agency processes and procedures for adjudicating an unsatisfactory PIV application.
- Be a U.S. citizen or U.S. national or hold a U.S. government security clearance.
- Have successfully completed the PIV Registrar training modules.

The **PIV Issuer** is the individual or entity that issues an identity credential to an Applicant following the positive completion of all identity proofing, background checks, and related approvals.

Federal Identity Management Handbook

The PIV Issuer should meet the following minimum standards:

- Be a government official and be designated in writing as a PIV Issuer
- Be a U.S. citizen or a U.S. national or hold a U.S. government security clearance
- Have successfully completed the PIV Issuer Training modules

The **PIV Digital Signatory** is the entity that signs the PIV biometric and cardholder unique identifier (CHUID) of the Applicant.

The PIV Digital Signatory should meet the following minimum standards:

- Be a government official and be designated in writing as a PIV Issuer
- Be a U.S. citizen or a U.S. national or hold a U.S. government security clearance
- Have successfully completed the PIV Issuer Training modules

The **PIV Authentication Certification Authority (CA)** is the CA that signs and issues the PIV Authentication Certificate of the Applicant.

The PIV Authentication CA should meet the following minimum standards:

- Participate in the hierarchical PKI for the Common Policy managed by the Federal PKI
- Conform to Worksheets 1-3 in X.509 Certificate and CRL Profile for the Common Policy

2.3.2.2 Training

All of the roles defined above should be implemented in an agency's identity-proofing process. Each role is unique and has its own requirements. Training should be provided to ensure that each role functions properly. Individuals who are designated for the roles identified above will require training in two areas:

- Agency-specific processes and procedures. These are the processes and procedures that are unique within each agency (for example, the method for adjudicating an unsatisfactory PIV application).
- PIV-specific processes and procedures. These are the processes and procedures that are unique to the PIV identity-proofing process (for example, the methodology for assessing the completeness of an Applicant's request or the steps involved in completing a PIV application form.)

2.3.2.3 Identity-Proofing and Registration Process Steps

This section describes the requirements for the role based identity-proofing and registration steps. Agencies can implement more stringent requirements as long as they follow the minimum requirements defined below.

1. The PIV Sponsor completes a PIV request for an Applicant. (Appendix C depicts a sample PIV request.)
2. The PIV Sponsor submits the request to the PIV Registrar and the PIV Issuer.

Federal Identity Management Handbook

3. The PIV Registrar confirms the validity of the PIV request.
4. After the request is validated, the Applicant completes an SF 85, OPM questionnaire (for non-sensitive positions) or its equivalent. (SF 85, OPM questionnaire is located at the following location, http://www.opm.gov/forms/pdf_fill/SF85.pdf)
5. The Applicant provides the completed form to the PIV Registrar.
6. The Applicant appears in person and provides two identity source documents to the PIV Registrar. At least one of the identity source documents should be a valid picture ID issued by a state or by the Federal Government.
7. The PIV Registrar visually inspects the identity source documents and validates them electronically as being unaltered and authentic. (If electronic means are unavailable, the PIV Registrar uses another means to authenticate the identity source documents.) The PIV Registrar also verifies that the picture on the identity source documents is of the Applicant.
8. If the PIV Registrar is able to validate the documents successfully, the Registrar records the following information for each of the identity source documents provided by the Applicant. The documents may also be scanned:
 - The title of the document
 - The document's issuing authority
 - The document's number, as listed on the document
 - The document's expiration date, if available
 - Any other information deemed necessary to confirm the identity of the Applicant
9. The PIV Registrar signs and files the record of the collected information.

The PIV Registrar is not required to keep a copy of the original documents, to reduce the likelihood that an Applicant's identity source documents are compromised.
10. The PIV Registrar compares the information on the PIV Request to the information provided on the SF 85 (or equivalent) and the identity source documents to ensure that the information is the same on all forms.
11. The PIV Registrar obtains and retains a copy of the facial image of the Applicant. The facial image shall conform to SP 800-73.
12. The PIV Registrar collects and retains all 10 fingerprints of the Applicant. Two of these fingerprints should be collected in accordance with the instructions in Section 4 of this document.
13. The PIV Registrar initiates a National Agency Check with Inquiries (NACI) on behalf of the applicant.

Agencies will need to define a specific adjudication process for when such investigations return unfavorable results.
14. The PIV Registrar notifies the PIV Sponsor and PIV Issuer of the results of the process.

Federal Identity Management Handbook

- If all steps have been completed successfully, the Sponsor and Issuer are notified that the applicant has been approved for a PIV card.
 - If any of the background checks are unsuccessful or if there are irregularities in the applicant's information, the Sponsor and Issuer are notified that irregularities have occurred.
15. The PIV Registrar uses a secure process to make the following information available to the PIV Issuer:
- Applicant's electronic photo
 - A copy of the results of the Applicant's background investigation
 - Other data associated with the Applicant (i.e., Applicant's name, affiliation, contact information)
16. The PIV Registrar should make the following information available to the PIV Digital Signatory via a secure process:
- Electronic biometric data for card personalization
 - Other data associated with the Applicant that is required for the generation of signed objects for card personalization
17. The PIV Registrar maintains the following information pertaining to the Applicant:
- Completed and signed PIV Request
 - Completed and signed SF 85 (or equivalent)
 - Information concerning the identity source documents collected in Step 8.
 - The results of the applicable background check
 - Copies of photo and fingerprints collected in Steps 11 and 12.
 - Any other relevant materials used to validate the Applicant's identity

Current employees with a valid background check on file do not require an additional background check. The PIV Registrar can notify the PIV Issuer that a credential can be issued to the Applicant if a valid background check is on file.

2.3.2.4 Issuance Steps

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

Agencies should develop a precise business process for distribution and confirmation of the PIV request and the approval notification. This is discussed below.

2. The PIV Issuer shall initiate the creation of a CHUID for the new PIV Card. The CHUID shall be made available to the PIV Digital Signatory through a secure mechanism.

Federal Identity Management Handbook

3. The Digital Signatory shall create digitally signed credential elements (biometric and CHUID) needed for the card personalization process, using the data supplied by the PIV Registrar and the newly assigned CHUID. The digitally signed credential elements shall comply with the relevant specifications in Sections 4.2.2 and 4.4.2. The signed credential elements shall be made available to the PIV Issuer.
4. The Applicant may be asked to provide a PIN, or the PIV Issuer may generate a PIN on the Applicant's behalf.
5. The PIV Issuer shall personalize the PIV card. The personalized PIV Card shall meet all of the technical and interoperability specifications in Section 4.
6. The Applicant may generate cryptographic key pairs for the PIV card and obtain the corresponding certificates from the PIV Authentication CA at this time. Alternatively, the Applicant may be supplied with a one-time authenticator for use in a subsequent certificate request to the PIV Authentication CA. In the latter case, the Applicant will generate key pairs at a local workstation rather than at the PIV Issuer location.
7. The recipient's name, issuer identity, card number, and possibly PKI certificate identification information shall be enrolled and registered with back-end data stores that support the PIV system. Depending on the infrastructure design, the back-end data stores may be centralized or decentralized.
8. The PIV Issuer shall control the creation and personalization of a new PIV card using the information provided by the PIV Registrar.

Card personalization can occur either during the actual issuance transaction (i.e., in the presence of the Applicant) or prior to the Applicant appearing in person to collect the card from the PIV Issuer. This is described in further detail below.

9. The Applicant shall appear in person to the PIV Issuer (or an authorized delegate) to collect the PIV card. Before the newly created PIV card is given to the Applicant, the PIV Issuer shall verify that the individual who collects the identity credential is indeed the Applicant through the following steps:
 - The individual shall present a state or Federal government-issued picture identity source document. The PIV Issuer (or an authorized delegate) shall validate that the picture and name on this source document match the picture and name on the newly personalized PIV card. Additionally, the PIV Issuer (or an authorized delegate) shall validate that the individual looks like the picture on the PIV card.
 - The PIV Issuer (or an authorized delegate) shall check that the fingerprint of the individual matches the biometric credential embedded in the PIV card.

It is important to note the requirement for the Applicant to appear in person to the PIV Issuer to receive the PIV credential. Agencies should plan their issuance strategies carefully in order to comply with this requirement. Agencies should base their decision on:

- Internal review of issuance infrastructure
- Issuance population
- Individuals designated as a PIV Issuer

Federal Identity Management Handbook

10. The PIV Issuer shall obtain a signature from the Applicant (now PIV cardholder) attesting to the Applicant's acceptance of the PIV card and related responsibilities.

This requirement is to ensure that the PIV cardholder has taken acceptance of the PIV card as well as been informed of the responsibilities involved in its ownership. PIV cardholders should be informed of the following:

- If their PIV card begins to wear (i.e., laminate coming loose, ink rubbing off, cuts/rips/tears occur in the card) they should return to the PIV Issuer immediately.
- If their PIV card is lost or stolen, they should notify the PIV Issuer immediately.
- If their PIV card does not operate properly when inserted into a logical or physical access reader, they should notify the PIV Issuer immediately.
- If any personal information changes, the PIV cardholder should notify the PIV Issuer immediately (i.e., changes in affiliation, name change, or other personal information changes).

As one final check the PIV Issuer may conduct a one-to-one fingerprint biometric check on the Applicant. Although this is not required in PIV I, agencies should consider implementing a method whereby the PIV Issuer conducts a one-to-one fingerprint biometric check between the Applicant's enrolled image and a live sample before issuing the card. This one-to-one check provides additional assurance that the individual who applied and was enrolled for a PIV card is the same individual who is being issued a PIV card, thus, increasing confidence in the Applicant's identity.

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

Agencies should develop a secure and timely scheme for notifying the PIV Sponsor and PIV Registrar of PIV credential personalization and issuance to a PIV cardholder. In circumstances where any of the steps are unsuccessful, agencies should follow internal policies and procedures for adjudication of an Applicant's PIV request.

12. The PIV Issuer shall be responsible for maintaining the following:

- Completed and formally authorized PIV Request
- The approval notice from the PIV Registrar
- The name of the PIV Applicant
- The credential identifier, such as an agency card serial number
- The expiration date of the identity credential
- The signed acceptance form from the Applicant.
- Records and controls for PIV card stock, to ensure that stock is only used to issue valid credentials.

Agencies should establish a business process and secure delivery method for all PIV-related documents. Agencies can implement a system-based model that provides all or part of the data and

Federal Identity Management Handbook

document management requirements for storage, notifications, and approval/disapprovals electronically. This can include web-based applications for use by the PIV Sponsor, PIV Registrar, and PIV Issuer functions. Alternatively, agencies could choose to implement a business process that is more manual in its functionality. This process would consist of documents stored in hard-copy form and notifications and approvals/disapprovals generated via e-mail or telephone communication from one role to another. Regardless of the exact business process implemented by the agency, the process should be auditable, secure, and provide for protection of the privacy the applicant's information privacy.

2.3.3 System-Based Model Example

The system-based model may be ideal for agencies that already have an automated identity management system. The system-based model allows accredited service providers to function in any of the roles described below. Additionally, accredited service providers may perform any of the processes describe below. The sections below summarize the roles, components, and processes of a typical system-based model.

2.3.3.1 System Based Roles

The PIV system based identity proofing process defines the following roles:

- Applicant
- Employer/Sponsor
- Approval Authority
- Issuing Authority (Issuer)

The **Applicant** is the individual to whom a PIV card will be issued once the PIV Registrar approves the application and the appropriate background checks have taken place. The Applicant must appear in person to the Employer/Sponsor or the Approval Authority or the Issuing Authority at least once prior to issuance of a PIV card.

In support of the application process, the Applicant should complete the following activities:

- Complete an SF 85 or equivalent
- Present two forms of identification from the list of acceptable documents listed on *I-9, OMB No. 1115-0136, Employment Eligibility*
- Successfully complete the Applicant training modules

The **Employer/Sponsor** is the individual who validates an Applicant's requirement for a PIV card and authorizes the Applicant's request.

The Employer/Sponsor should meet the following minimum standards:

- Be a government official and be authorized in writing by the agency to request a PIV card
- Have valid justification for requesting a PIV card for an Applicant
- Be in a position of responsibility for the agency

Federal Identity Management Handbook

- Have already been issued a valid PIV card
- Have successfully completed the Federal PIV Sponsor training modules

The **Approval Authority** establishes the organization chain of command within the identity management system (IDMS). This individual also manages the scope of the chain of trust between the enrollment process, the IDMS, card production and activation. This individual manages the entire IDMS and is also responsible for designating those individuals who will perform the duties of the Employer/Sponsor. Additionally, the Approval Authority should make sure that no single individual/role has the capability to issue a card without the participation of another individual and that there are at least two different individuals participating in the process at all times. The Approval Authority should be responsible for validating and auditing all of the checks that are conducted by the IDMS.

The Approval Authority should meet the following minimum standards:

- Be a government official and be designated in writing as an Approval Authority
- Be a U.S. citizen or a U.S. national or hold a valid U.S. Government security clearance
- Be in a position of responsibility for the agency
- Have already been issued a valid PIV card
- Have successfully completed the Federal Approval Authority training modules

The **Issuing Authority (Issuer)** is the individual or entity who activates and issues a PIV card to an Applicant following the positive completion of all identity proofing, background checks, and related approvals. The Issuing Authority is responsible for ensuring that a one-to-one biometric check of the Applicant's enrolled fingerprint biometric image and an image presented by the Applicant before credential issuance is conducted.

The Issuing Authority should meet the following minimum standards:

- Be a government official and be designated in writing as an Issuing Authority
- Be a U.S. citizen or a U.S. national or hold a U.S. government security clearance
- Have successfully completed the Issuing Authority Training modules

2.3.3.2 Components

Certain components are associated with the system-based model. These components automate some of the tasks that are completed manually in the role-based model. A description of these components follows.

The Approval Authority maintains the **IDMS**. The IDMS contains records, including all documentation for all issued PIV cards. The card management system within the IDMS should track the status of a PIV card throughout its entire lifecycle, including the production-request, personalization and printing, activation and issuance, suspension, revocation, and destruction phases. Additionally, the IDMS performs the identity proofing, verification, and validation of an Applicant prior to PIV issuance. The biometric database within the IDMS has the capability to do a one-to-many fingerprint biometric

Federal Identity Management Handbook

search on all Applicants in the system to ensure that no Applicants have already been issued a PIV card and are requesting additional PIV cards fraudulently. In accordance with HSPD-11,⁵ the IDMS will have the capability to conduct identity verification and validation processes using government-wide databases and services. In addition, the IDMS should provide the following services:

- Notify Applicants of the status of or be available to be queried by the applicant for their PIV requests
- Notify the Employer/Sponsor of or be available to be queried by the applicant for the PIV request
- Notify or be available to be queried by the Employers/Sponsors, Approval Authorities, and Issuing Authorities to see if a credential is still valid

The IDMS should contain all data records and be responsible for providing the Applicant's data record that will be used by the Card Production and Personalization system. The IDMS should provide the card personalization information via secure means.

The **Enrollment System** initiates the chain of trust for identity proofing by confirming employer sponsorship, validating identity documentation, and binding Applicants to their biometric data, and validating identity documentation. The enrollment system provides the IDMS with all of the identity documentation and forms that an Applicant completes prior to PIV card issuance. Although not defined in FIPS 201, agencies will have to establish an Enrollment Official to be responsible for operating the enrollment system. Because this individual will have access to Applicants' personal information and biometric data, the Enrollment Official should have a valid U.S. Government security clearance and be trained to operate the enrollment system.

The **Card Production and Personalization System** personalizes and prints PIV credentials after the IDMS has approved such actions. Additionally, the IDMS should provide the following services:

- Maintain full inventory control of blank card stock, consumables, and manufacturing materials
- Maintain a list of IDMSs that can submit PIV requests for card production
- Maintain a list of Issuing Authorities that can activate and issue PIV cards
- Provide electronic acknowledgement of IDMS requests for PIV card production
- Notify the IDMS of successful/unsuccessful production of a PIV card
- Allow only approved individuals to access an Applicant's card personalization information

These systems are essential in maintaining the chain of trust. Therefore, for each of the systems listed above, there should be a documented business process, a security evaluation, and a security policy.

2.3.3.3 Issuance Steps

This section describes the requirements for the system-based identity-proofing and registration process defined in FIPS 201. Agencies can implement more stringent requirements as long as they follow the minimum requirements defined below. Figure 1 illustrates the process. All actions taken and systems associated with those actions should be auditable and secure.

⁵ Homeland Presidential Security Directive 11 (HSPD-11) defines comprehensive terrorist-related screening procedures.

Federal Identity Management Handbook

1. Employers/Sponsors are pre-registered in the IDMS
2. The Applicant provides a formal PIV request and a minimum of two forms of acceptable identity documentation from *I-9, OMB No. 1115-0136, Employment Eligibility* to the Employer/Sponsor. At least one of the documents must be a valid picture ID issued by a state or by the Federal Government.
3. The Employer/Sponsor approves the request.
4. The Applicant appears for enrollment and provides the same documentation as provided to the Employer/Sponsor.
5. The Applicant's identity documents are inspected and verified. If available, an electronic method should be used to check the validity of the identity documents.
6. The Employer/Sponsor's approval is verified.
7. Fingerprints and a photograph of the Applicant are taken. The fingerprints and photograph must meet the standards defined in Sections 4.1.1.1.1 and 4.3 of this document.
8. The Applicant's supporting documents are scanned into the system electronically.
9. The Applicant's completed electronic enrollment package (scanned documents, biometric samples, and digital photograph) are digitally signed and forwarded to the IDMS.
10. The IDMS verifies the integrity of the enrollment package by confirming completeness and accuracy and that the digital signature is valid.
11. The IDMS confirms that the Employer/Sponsor is valid and approved the request.
12. The IDMS performs a one-to-many fingerprint biometric search to ensure that the Applicant is not already enrolled in the system.
13. The IDMS performs appropriate identity verification and validation through government-wide databases in accordance with HSPD-11 (HSPD-11 can be found at the following location, <http://www.whitehouse.gov/news/releases/2004/08/print/20040827-7.html>).
14. Once the IDMS has successfully completed steps 10–13, the Approval Authority approves card production for the Applicant.
15. The IDMS sends the information necessary for card personalization to the card production and personalization system.
16. The card production and personalization system personalizes and prints the PIV card.
17. Prior to issuing the PIV card to the Applicant, a one-to-one fingerprint biometric check is conducted against the IDMS record to ensure that the person who was enrolled in the system is the same individual being issued the PIV card.
18. The Issuer activates the PIV card.

2.3.4 Suspension, Revocation, and Destruction

Certain circumstances require a PIV card to be suspended, revoked, or destroyed. Agencies will therefore need to create a card registry that is capable of displaying the status of PIV cards in real time.

Agencies may suspend credentials for various reasons, but most commonly such suspensions will be temporary (for example, when an individual takes maternity leave). In all likelihood under this circumstance agencies will not want to revoke the PIV card. Agencies will therefore need to develop reinstatement policies for situations in which an agency suspends a PIV card with the intention of reinstating the card later. It is recommended that agencies do the following:

- Suspend or deactivate the logical data elements.
- Update the card registry to indicate the PIV card has been suspended.
- Store the suspended card in a secure location.
- Establish rules for the maximum amount of time that a PIV card can be suspended. For example a suspended PIV card cannot be reinstated if the individual has been away from the agency for more than 6 months.
- Ensure that a valid NACI, NAC, or other national security community investigation required for Federal employment is on file before card reinstatement.

Example circumstances in which an agency will want to revoke a PIV card include the following:

- The card has been compromised (i.e., stolen or lost).
- An agency has terminated employment of an individual.
- An individual has received a promotion, thus requiring new information to be printed on the card.

The process for revoking a PIV card could include the following:

- Deactivate the logical data elements
- Update the card registry to indicate that the PIV card has been suspended
- If the card is available, destroy the PIV card

2.3.5 Reissuance to Current PIV Cardholders

Reissuance will occur when a PIV card has expired or an individual has lost a PIV card. Reissuance requires the Issuing Authority to perform the following:

- Query the IDMS to ensure that the PIV credential is not expired.
- Verify the individual requesting reissuance of a PIV card by conducting a one-to-one fingerprint biometric match to data stored in the IDMS
- Verify the photograph in the IDMS is the person who is requesting a PIV card.
- Recapture biometrics.
- Issue a new credential and update the IDMS record for the individual.

Federal Identity Management Handbook

- Digitally sign the biometrics and new credential record.

Agencies will need to develop specific business processes beyond what is described above for the suspension, revocation, reissuance, and destruction of all PIV cards. The processes should be secure and protect the privacy of PIV cardholders. Additionally, agencies should provide proper training to those individuals responsible for performing each of the processes and training on who will update the card registry, how often, and how. Because of the heightened security requirements throughout the Federal Government, it is recommended that agencies implement a method that allows real-time updating of the card registry.

2.4 Privacy Requirements

2.4.1 Protecting Personal Privacy

During the FIPS 201 identity-proofing and issuance process agencies will have certain responsibilities for collecting, validating, transmitting, and storing the PIV Applicant's personal information. One of the stated objectives of HSPD-12 is that the PIV system is to protect the personal privacy of all cardholders. To accomplish this, agencies must put certain privacy controls in place. These controls will help ensure that PIV information is collected, transmitted, stored, and used in a secure manner that does not affect the PIV applicant's right to privacy.

Several Federal guidelines and policies are currently in place that apply to the protection of an individual's privacy, including OMB Memorandum M-05-08, the E-Government Act of 2002, the Privacy Act of 1974, OMB Memorandum M-03-22, and NIST SP 800-73. Agencies must also adhere to the requirements described below when implementing FIPS 201.

2.4.2 Agency Requirements

FIPS 201 requires the transfer and storage of a PIV applicant's personal information. Every agency has an obligation to their employees to protect their privacy. FIPS 201 mandates that agencies do the following.

2.4.2.1 Senior Agency Official for Privacy

Agencies must assign an individual to be the senior agency official for privacy. This individual may not assume any other operational role in the PIV system (i.e., Registrar, Issuer, CA).

The senior agency official for privacy should be the lead for implementing PIV privacy policies and agency-specific policies and ensure that they are being applied and maintained in a consistent manner throughout every phase of FIPS 201 implementation (design, development, implementation, and post-implementation). The senior agency official for privacy should have intimate knowledge of Federal and agency-specific privacy policies and best practices.

OMB Memorandum M-05-08 Designation of Senior Agency Officials for Privacy requires that by March 11, 2005, executive-level departments and agencies designate a person to be responsible for agency-wide privacy issues. Agencies may find it useful to let the senior agency official for privacy assume the duties of maintaining the privacy requirements of FIPS 201. In some agencies, a single individual may already be responsible for privacy related issues. In other agencies, multiple individuals

Federal Identity Management Handbook

may be responsible for privacy issues. These agencies will have to designate a single individual as the senior agency official for privacy. Senior agency officials for privacy can have duties unrelated to their responsibilities for FIPS 201.

2.4.2.2 Privacy Impact Assessment

Agencies must conduct a Privacy Impact Assessment (PIA) on those systems and processes that support the transmission and storage of a PIV Applicant's information in identifiable form (IIF). IIF is data in an IT system or online collection (i.e., a web-application) (1) that directly identifies an individual (name, address, social security number, telephone number, e-mail address) or (2) which an agency intends to use in conjunction with other data elements to identify an individual (indirect identification).⁶ An example of an indirect identification data element is the CHUID, which contains the Federal Agency Smart Credential Number (FASC-N). The CHUID and FASC-N are described further in Section 4.1.3.2.

Agencies may also have to maintain an applicant's information non-electronically. The PIA should also assess the security and privacy of information stored in physical form (paper records). Many agencies currently store employee records or some subset of their records in storage rooms or warehouses. Such storage can be cumbersome, difficult to manage, and a security vulnerability. Agencies currently maintaining applicant information in physical form should consider implementing an electronic method for maintaining an applicant's information. When this is not feasible, the PIA must include information stored in physical form.

The senior agency official for privacy should have direct oversight of the PIA. PIAs should be conducted in accordance with OMB M-03-22, which defines the conditions and requirements for conducting a PIA. Agencies should use the PIA internally to identify any weaknesses or flaws in protecting the privacy of its employees. OMB, M-03-22 can be found in its entirety at <http://www.whitehouse.gov/omb/memoranda/m03-22.html>. Following is a summary of the information that should be included in a PIA.⁷

- What information is to be collected (nature and source)
- Why the information is being collected (e.g., to determine eligibility)
- Intended use of the information (e.g., to verify existing data)
- With whom the information will be shared (e.g., another agency for a specified programmatic purpose)
- What opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent
- How the information will be secured (e.g., administrative and technological controls)
- Whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a

⁶ OMB Memorandum, M-03-22, *Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, OMB, September 26, 2003

⁷ Ibid.

Federal Identity Management Handbook

PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.

2.4.2.3 Full Disclosure

Agencies are required to write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected. Additionally, agencies must clearly explain the following to an Applicant:

- What information will be collected and how the information will be collected
- What information will be stored and how it will be stored
- What information will be transmitted and how it will be transmitted
- What information will be used and how it will be used
- Who will have access to the information
- How the information will be protected

Many departments and agencies currently have policies that inform an Applicant as to what information will be collected as a condition of their employment. The results of the PIA should assist agencies in identifying and communicating this information to applicants. Agencies may find it useful to produce pamphlets, briefings, and handouts that describe what applicants need to know about the collection, transmission, use, and storage of their IIF. Additionally, agencies will find it beneficial to educate users on all aspects of the FIPS 201 implementation, not just the privacy issues. User acceptance will aid greatly in a successful implementation.

2.4.2.4 Privacy Act of 1974

Agencies must ensure that a PIV Applicant's information is managed in a manner consistent with the Privacy Act of 1974. The Privacy Act of 1974 defines the processes, terms, rules, and requirements for maintaining the privacy of individuals' records. (For the full text of the Privacy Act of 1974, <http://www.usdoj.gov/foia/privstat.htm>).

2.4.2.5 Appeals Process for Denied/Revoked Credentials

Agencies must allow an Applicant who has been denied a PIV card or a cardholder whose card has been revoked a method to appeal.

Agencies should ensure that the adjudication method they establish defines this process precisely and identifies the individuals within an agency who should be involved in the appeal of a denied or revoked card. Generally, individuals who know that they should not be issued a PIV credential or know that it is proper for their credential to be revoked will not appeal such actions. Only those individuals who feel that an error has occurred will appeal. The appeal may reveal that an error was made in the identity proofing and registration process. The appeal process gives the agency an opportunity to correct such errors.

2.4.2.6 Legitimate Need to Access Systems

Only individuals with a legitimate need to access the systems in which an applicant's IIF is stored and maintained can be allowed to access those systems. Such systems include all databases and applications that contain an applicant's information.

The definition of who has a legitimate need to access the agency's PIV system will differ from agency to agency. For example, some agencies may allow contractors to access their systems, while other agencies will allow only government personnel to access their systems. Regardless, every agency must ensure that only individuals whose immediate duties require them to access PIV systems should be able to access those systems. Agencies should establish and implement a clear and auditable set of business processes to control system access. Additionally, the system implemented by an agency and the PIA must define the procedures for individuals to access and review any data stored in the system to ensure the accuracy of the data.

2.4.2.7 Consequences for Violating PIV Privacy Policies

Agencies must define the consequences of violating the PIV privacy policies.

After defining the consequences of violating PIV privacy policies, agencies should publish their privacy rules so that all individuals within that agency are aware of the rules and the consequences for violating them. Different agencies can have different rules defining the consequences for violating PIV privacy policies. All individuals within an organization are capable of violating privacy rules. Some things that every agency should consider when defining the consequences include:

- The severity of the violation
- The number of times a violation has occurred
- Whether the violation was malicious

2.4.2.8 Technologies and Systems

Agencies must ensure that the technologies and systems used to collect, validate, transmit, and store an applicant's information are in compliance with the PIV privacy policies and allow for continuous auditing.

The requirement to audit the technologies and systems used to implement FIPS 201 is important for ensuring the privacy of the agency's employees. The PIA should identify the technologies and systems that will be used by agencies. Agencies should institute business processes that address how and when a system should be audited. Continuous auditing implies that the technologies and systems used to implement FIPS 201 can be audited in real time. When real-time auditing is not possible, agencies should define exactly when and how auditing will occur.

2.4.2.9 NIST SP 800-53

Agencies must, where applicable, use the security controls defined in NIST SP 800-53 to assist in compliance with the PIV privacy policies.

Federal Identity Management Handbook

SP 800-53 identifies and defines security controls that agencies should implement to protect their information systems. SP 800-53 was published on February 28, 2005. The full text version can be found at <http://csrc.nist.gov/publications/> and <http://csrc.nist.gov/sec-cert>.

2.4.2.10 Sustaining PIV Privacy Policies

Agencies must ensure that the technologies and systems used to collect, transmit, store, and use an PIV applicant's information sustain and do not erode the PIV privacy policies. Specifically, agencies must employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored in the integrated circuit chip (ICC) of a PIV card. Agencies will have to include this requirement in their acquisition strategy. (More information concerning technologies that can protect the information stored on a PIV card can be found in Section 4.7.2.)

This requirement means simply that agencies should implement technologies and systems that adhere to the privacy guidelines outlined in this section and do not interfere or impede with the privacy requirements.

2.4.2.11 Summary

Privacy protection must be built into every process associated with FIPS 201 and the PIV I and PIV II processes. Agencies should view privacy protection not as a one-time implementation requirement but as a function that should be monitored and maintained throughout the life of their FIPS 201 implementation. Agencies have many policies, guidelines, and best practices to aid them in implementing a FIPS 201-compliant system that protects cardholder privacy. Agencies may choose to implement privacy policies and best practices in addition to those mandated by FIPS 201.

2.5 PIV Card Lifecycle

2.5.1 Managing the PIV Card Lifecycle

How to manage card lifecycles is one of the fundamental elements of a secure identity management system. Lifecycle management encompasses the entire life of a smart card, beginning at the pre-issuance stage, when an agency provides the card specifications to a card manufacturer, and ending at termination, when the card is deactivated or retired.

Because smart cards contain processors that are capable of running several different applications, it is a best practice to provide lifecycle management for these applications. Therefore, the card lifecycle management methodology endorsed by an agency may also include management of all applications that reside on the smart card.

Smart cards are a dynamically programmable technology that can communicate with card readers and back-end repositories. Regular maintenance must be performed so that the card continues to perform effectively. A successful card lifecycle management methodology enables an agency to maintain control over its card population and monitor each card's usage throughout that card's life.

The *Government Smart Card Handbook*⁸ includes a section on card lifecycle management architecture that agencies can use to supplement the key design components described in the following subsections. Both of these documents will assist agencies in the creation of an implementation process. The *Handbook* is available at: <http://smart.gov>.

2.5.2 Suggested Card Lifecycle Management Methodology

FIPS 201 includes information about card lifecycle management, but it does not stipulate specific requirements. The information is based on best practices culled from agency deployments of smart cards. Therefore, an agency can choose its own method for managing card lifecycles. The process flow shown in Figure 1 is an example of a card lifecycle methodology. Stages one, three, four, and five are referenced in FIPS 201. Application management, data management, and certificate management correspond to PIV card maintenance in FIPS 201. Reissuance, revocation, and termination are all components of what FIPS 201 refers to as PIV card termination. Although FIPS 201 does not comment on the pre-issuance stage, it is included in the process flow to provide agencies with a perspective on the entire card lifecycle.

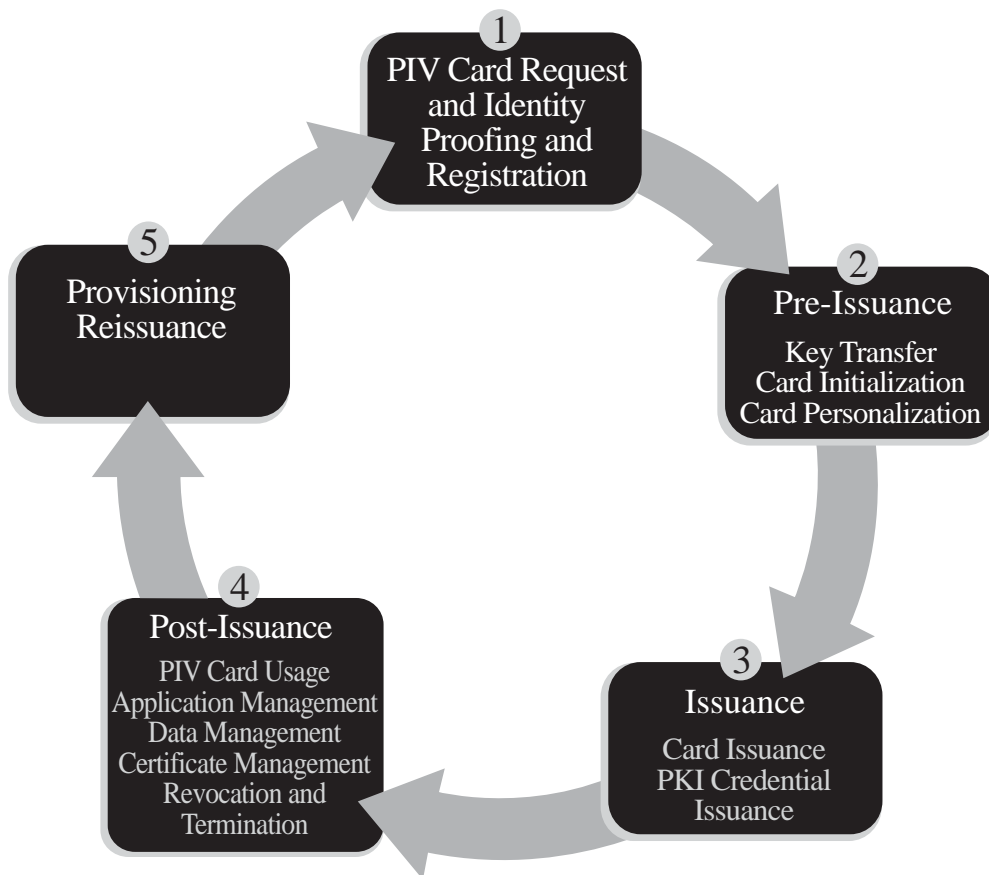


FIGURE 1. SAMPLE CARD LIFECYCLE METHODOLOGY

⁸ *Government Smart Card Handbook*, General Services Administration, February 2004.

2.5.3 Card Lifecycle Management Implementation

2.5.3.1 Key Technical Specifications

The card lifecycle management marketplace is fairly mature. Many commercial-off-the-shelf (COTS) products are offered by a variety of vendors. Many of the available solutions are based on a modular platforms, providing government agencies with the ability to customize an integrated architecture or simply build a stand-alone solution. There are, however, three principal components to a card lifecycle management system:

- Card management
- Application management
- Key management

The card management component is responsible for the card issuance process and the lifecycle management of smart cards. Additionally, it generates statistics and data regarding the installed base of cards. These queries and reports are reviewed to detect any anomalies in the system.

The application management component is responsible for maintaining the applications hosted on smart cards. In addition to monitoring the applications, application management also interacts with application providers whenever application-specific information needs to be exchanged.

The key management component is responsible for the implementation of security procedures for the generation, secure storage, and distribution of electronic encryption keys. Electronic keys are used to encrypt and decrypt data and to verify and authorize trusted parties through the use of digital certificates.

2.5.3.2 Card Lifecycle Stages

Three primary stages are associated with card lifecycle management: pre-issuance, issuance, and post-issuance. The following sections describe specific processes associated with each stage.

2.5.3.2.1 Pre-Issuance Stage

In the pre-issuance stage, a Federal agency is responsible for creating a specification that documents the requirements for manufacturing and delivering smart cards. The specification includes both technical and process requirements. The technical requirements include a description of the key management process, by which the agency transmits the keys to the card manufacturer for storage on the card. The process requirements include a description of the security controls that must be implemented once the card order is ready to guarantee delivery to the issuing agency. For example, a numbering scheme could be introduced for card manufacturers to follow so that duplicate cards are not issued. A secure method of delivery also ensures that the card stock has not been tampered with and meets the FIPS 201 card body specifications.

It is important to note that while managing card lifecycles is not mandatory, the Federal Government is attempting to achieve a uniform pre-issuance process. The impetus for a standardized process is the promotion of a common card platform, with which all vendors would be able to comply. Agencies that design their card lifecycle management processes in accordance with standards such as FIPS 201 will

Federal Identity Management Handbook

be free to select any compliant smart card available on the market, since each compliant manufacturer would offer compatible product suites. Moreover, when agencies issue standardized pre-issuance specifications, card interoperability among agencies will presumably increase beyond what will already be achieved by the integration of FIPS 201-compliant cards.

Several processes must occur during card manufacture to configure a smart card. The two most critical processes are card initialization and card personalization.

At card initialization, the manufacturer performs functions such as programming the ICC that resides on the smart card, loading the operating system with the card serial number and security keys, and reserving areas of memory for photos, digital signatures, and biometrics. NIST SP 800-73, the technical companion to FIPS 201, provides detailed requirements for implementing the initialization functions.

During card personalization, the card topology is configured according to the issuing agency's criteria and the cardholder's information is programmed into the chip and printed on the card's surface, associating the card uniquely with the cardholder. In addition, the cardholder's physical and logical access-control privileges are instantiated to the card. Again, agencies are advised to reference NIST SP 800-73 as a technical implementation supplement.

2.5.3.2.2 Issuance Stage

Card management enters the issuance stage after a card is manufactured and delivered to the issuing agency. The issuing agency is responsible for distributing the personalized cards to the correct cardholders. An agency must choose whether to distribute cards from a central location or from regional issuing stations. Multiple factors influence this decision. These factors include the cardholder's location, whether multiple issuing authorities are available, and the definition of logistical support for card distribution. It should be noted that regional issuance has a higher security risk. To evaluate appropriate risk and cost factors, an agency should develop a business process to determine how to issue its cards.

Services and Support

Before a card lifecycle management system has been selected and deployed, an agency should carefully review the terms of its contract with the vendor to determine that training and maintenance are addressed. The provision of adequate training in combination with ongoing support and maintenance is a major factor in the successful implementation of any information technology system, even one composed of COTS products.

Training

The contractor must be able to provide end-user training on the card lifecycle management system to agency personnel as required. Typically, training classes are both formal, consisting of approximately 4 days of instruction, and informal, consisting of on-site "desk-side coaching" sessions. Both technical training and user training should be available. It is also recommended that training on day-to-day operations be provided to system operators and administrators to ensure that they have a thorough understanding of the systems and related components they will be responsible for managing.

The training supplier must be able to provide lesson plans and training manuals that include the type of training to be offered and a list of reference materials.

Support and Maintenance

Agency staff or a contractor should be able to perform maintenance of the card lifecycle management system, including supporting software and hardware. The same personnel should provide periodic resolution support for any issues and ongoing training as required.

The contractor should also be able to provide both onsite and offsite help desk support according to the agency's requirements. To facilitate this effort, the contractor should write and publish a help desk manual for the agency, to serve as a reference guide when immediate action must be taken to resolve a system malfunction. The contractor may also be required to publish help desk software that can track trouble calls, dispatch trouble tickets and repairs, import and export data, and create tracking reports. Other contractor duties may include monitoring the system and preparing regular reports, such as operational readiness reports or monthly status reports.

2.5.3.2.3 *Post-Issuance Stage*

The post-issuance stage begins as soon as the cardholder receives the card and begins to use it. During this stage, the agency is responsible for managing the card applications, data, and applets to ensure that only an authorized user is using the card and that the card is being used within the scope of the user's authority.

Certificate management for PKI systems is part of both the issuance stage and the post-issuance stage. The PKI CA is responsible for properly vetting each certificate request before creating, signing, and publishing the cardholder's certificate. This process occurs during identity proofing and enrollment, which immediately precede card issuance. During the post-issuance stage, the chain of trust established between the agency CA and any dependent parties must be maintained diligently to ensure the secure exchange of digital certificates. Additionally, as certificates expire, cardholders must be able to submit requests for renewed certificates.

Cardholders may lose or misplace their cards or forget the PIN or password required to authenticate to the card, or one of the applications running on a card may cause it to fail. Agencies should design suitable contingency plans to address these situations. Business continuity and the ability to accommodate access control issues are key drivers for each Federal agency. Managing risk by implementing a card management system enables agencies to avoid reissuing a card to an employee or contractor who no longer needs a card and to alert the access control system that a cardholder no longer requires access. It also enables a legitimate user to reset a password easily. This effort should focus on creating procedures for agency card administrators, not on the technical components associated with each issue.

Particular attention should be given to developing a process that enables the agency to prove that the cardholder reporting the lost or faulty card is in fact the cardholder to whom the card was issued. To address this issue, card management systems typically store information in the cardholder's file that the cardholder can remember easily but that is difficult for somebody else to guess. For example, the card-issuing authority may ask that cardholders provide their mother's maiden name before receiving a replacement card.

In the event that a card is lost, stolen, or malfunctioning, procedures should be established for the cardholder to notify the organization (or personnel) responsible for card management so that the original card can be deactivated and the cardholder can be issued a replacement card. For example, an

Federal Identity Management Handbook

agency might first update its revocation list by adding the card's identification number so that all possible fraudulent activity can be prevented. Next, the agency would access the demographic data, collected when the cardholder was enrolled and stored in a cardholder database, and process a request for a replacement card. This process is defined in Section 5.2.2.1 of FIPS 201.

Finally, if the cardholder's job changes or if the cardholder leaves the agency entirely, it is likely that card privileges will also change. To prevent a cardholder's card from being used inappropriately, the issuing agency should establish procedures for the timely deactivation of the card and adhere to best practice methods for recovering the card itself. This way, an agency can be assured that only authorized active cards are in circulation.

3. PIV - Validation, Certification, and Accreditation

PIV validation, certification, and accreditation is a quality assurance process that defines and evaluates risk, establishes mitigation and contingency plans to control risk, and assesses the overall vulnerability of business and IT processes. The process is comprehensive and includes an assessment of mission and operational requirements, key stakeholder participation, technical constraints, and security and deployment issues. The process requires that all individual functions that assume responsibility or risk be identified and accredited.

To determine whether individual PIV components are certified, agencies can use public information about vendor compliance and the NIST FIPS 201 Reference Implementation (described in Section 5.6). For example, when an agency prepares a purchase of PIV client applications, it can require that the vendor product perform satisfactorily with the PIV Reference Implementation. By doing so, an agency will not have to test a PIV client application on its own to determine whether it complies with FIPS 201 and SP 800-73. However, an agency should conduct its own independent testing on candidate products to ensure compatibility and interoperability with the agencies own environment. Because different agencies will comply with the PIV requirements in different ways, however, the PIV validation, certification, and accreditation process will require additional work by each agency. The process must consider all of the factors specific to an agency's particular PIV system.

3.1 FIPS 201 Requirements

To identify all of the risks associated with a PIV system, PIV validation, certification, and accreditation should be conducted before the go-live production decision. Agencies should create a schedule that adheres to OMB's implementation timeline for PIV I and PIV II compliance. The PIV I and PIV II identity-proofing, registration, issuance and maintenance process also requires accreditation by the department or agency Inspector General. Agencies should plan to make this a key component of their PIV implementation plans. Based on the results of the certification and accreditation process, the agency official can decide whether to authorize use of the agency's PIV system. This decision acknowledges and accepts the risks to an agency's personnel and assets inherent in PIV system use.

HSPD-12 established a benchmark requirement for the development of a PIV certification and accreditation process. All PIV system issuers, related IT systems, and components, including the PIV card, cryptographic modules, card readers, and middleware, must be independently certified for PIV system accreditation. The primary PIV components and their corresponding validation requirements are summarized in Table 1.

Table 1. PIV System Components and Validation Requirements⁹

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

In FIPS 201, NIST declared an intention to define PIV card accreditation criteria and establish a government-wide program to certify PIV card issuers.¹⁰ The benefits of such a program are very clear, as it will in effect standardize the accreditation criteria and absorb a lot of the responsibility that agencies would otherwise have in the accreditation process. Until such a program is established, agencies will have to continue self-certification.

3.2 NIST SP 800-37

Fortunately, guidance is available. FIPS 201 requires the use of NIST SP 800-37 for certifying and accrediting PIV systems. Figure 2 illustrates the four primary components of the certification and accreditation process outlined in SP 800-37 and details the major tasks associated with each component.

⁹ FIPS PUB 201, op. cit., p. 66.

¹⁰ Ibid.

Certification and Accreditation Methodology Overview

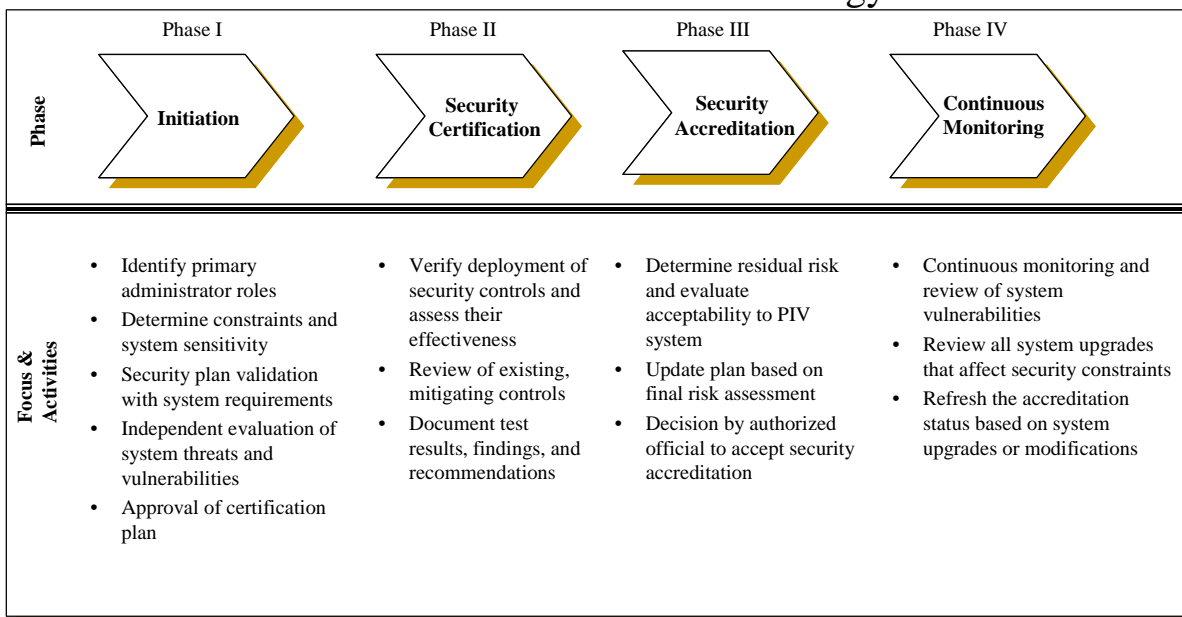


FIGURE 2. CERTIFICATION AND ACCREDITATION METHODOLOGY OVERVIEW

Phase I, Initiation, is when the primary roles in the process are identified and documented. The activities of each role are reviewed and areas of risk are outlined. A detailed review of the process is completed and threats and vulnerabilities are identified.

In Phase II, Security Certification, existing mitigation and contingency plans are reviewed and security controls assessed for their effectiveness.

During Phase III, Security Accreditation, plans are updated based on the final risk assessment and the decision is made by the authorized official to accept security accreditation.

Phase IV, Continuous Monitoring, incorporates a process-monitoring component. All systems, processes and security checkpoints are routinely reviewed and refreshed as needed.

3.3 Summary

The certification and accreditation process conducts a thorough review of an agency’s PIV system design and validates its findings. By establishing a consistent review of security controls and identifying risks associated with mission critical issues, agency officials will be able to make educated decisions that are based on reliable information.

4. PIV II - Front-End Subsystem

4.1 Physical PIV Card Requirements

Individuals within the Federal Government who are responsible for credentialing their employees may have different views on the appearance of their agency's credentials. FIPS 201 attempts to satisfy different agency requirements by providing a baseline specification to which the PIV credentials must adhere, while at the same time allowing for the inclusion of optional elements on the card. This enables agencies to customize their PIV credential to meet agency-specific needs, while at the same time adhering to the common PIV requirements defined in FIPS 201. This section summarizes the specifications for a FIPS 201-compliant PIV card, including the topography, security features, ICC features, and physical features.

The specifications include the physical characteristics of the card, commonly referred to as the *card body*. The prominent characteristics of a card body are the card's dimensions (width and height), thickness, and topology. The reason for defining common physical characteristics is so that PIV cards can be visually recognizable and accepted as well as generally behave in a similar manner. A PIV credential must also comply with applicable International Standards Organization/International Electrotechnical Commission (ISO/IEC) standards, summarized in Section 4.1.2.3. These standards are established to support global interoperability such that independent implementations based on an open standards should be interoperable.

This section also discusses the visual elements included in the topology of the card and the data elements included in the credential's ICC. A PIV card is imprinted with the cardholder's name, photograph, and other identifying information. The cardholder's agency or department affiliation is also printed on the card. The process of imprinting specific cardholder information and writing data to the ICC is called *card personalization* and occurs before the card is issued.

The FIPS 201 card specification also covers the machine-readable electronic components of the card. These components enable data on the card to be read and interpreted electronically. Examples of optional components that can be implemented on a PIV credential include a magnetic stripe (magstripe), barcodes, and optical technology.

FIPS 201 lists certain mandatory physical, topographical, and electronic elements. An agency can also choose to include several optional elements. The following sections provide further detail and recommendations for the physical design and characteristics of a PIV card.

4.1.1 Physical PIV Card Topology

This section lists the mandatory and optional topology elements of a PIV card. A PIV card must include certain elements on both the front and the back of the card. These elements are identified by zone. Table 2 and Table 3 identify the mandatory and optional zones on the front and back of the PIV card. The requirements for each element are described in the following sections.

Federal Identity Management Handbook

Table 2. PIV Card Topology Elements (Card Front)

Mandatory (Y/N)	Zone	Description	Data Format
Y	1	Photograph	Minimum 300 dpi
Y	2	Name	Minimum 10pt/arial font
N	3	Signature	
N	4	Agency specific text area	Agency discretion
N	5	Rank	Agency discretion
N	6	Portable Data File (PDF) two-dimensional bar code	IAW applicable AIM standards
Y	7	Reserved space for ICC	
Y	8	Employee Affiliation	6pt/arial/bold font
N	9	Header	6pt/arial/bold font
Y	10	Agency Name, Department, and/or Organization	6pt/arial/bold font
N	11	Agency Seal	20x20 mm, minimum 65% brightness/25% contrast
Y	12	Footer	6pt/arial/bold font
N	13	Issue Date	YYYYmmmdd, 6pt/arial/bold font
Y	14	Expiration Date	YYYYmmmdd, 6pt/arial/bold font
N	15	Color-Coding for Employee Affiliation	
N	16	Photo Border for Employee Affiliation	
N	17	Agency Specific Data	6pt/arial/bold font

Table 3. PIV Card Topology Elements (Card Back)

Mandatory (Y/N)	Zone	Description	Data Format
Y	1	Agency Card Serial Number	6pt/arial/bold font
Y	2	Issuer Identification	6pt/arial/bold font
N	3	Magnetic Stripe I	ISO 7811-6
N	4	Return To Information	5pt/arial/normal font
N	5	Physical Characteristics	6pt/arial/bold font
N	6	Additional Language for Emergency Responder Officials	5pt/arial/normal font

4.1.1.1 Mandatory PIV card elements

The seven mandatory elements that must be printed on a PIV card are:

- Photograph of the PIV cardholder (front of card)
- Name of the PIV cardholder (front of card)
- Employee affiliation of the PIV cardholder (front of card)
- Name of the agency, department, and/or organization with which the PIV cardholder is affiliated (front of card)
- Expiration date of the PIV card (front of card)
- Agency card serial number (back of card)
- Issuer identification (back of card)

The requirements for each visual element are described below. The placement and formatting for each mandatory element are shown in Figure 3 and Figure 4.

4.1.1.1.1 Front¹¹

Zone 1 – Photograph: The photograph should generally be placed in the upper left corner and be a full frontal pose, from the top of the head to the shoulders. The resolution must be a minimum of 300 dpi. The recommended dimensions are 37.0 x 27.75 mm, which is a .75 aspect ratio (width divided by height). The background for the photograph should follow recommendations set forth in SP 800-76.

Zone 2 – Name: The cardholder’s full name, or pseudonym when applicable under law, must be printed directly under the photograph in capital letters in at least a 10-pt font. The format for the name field should be last name, first name, middle initial. The dimensions of this zone are 8.5 x 49.0 mm.

¹¹ Ibid.

Federal Identity Management Handbook

Zone 7 – ICC: This space is reserved for a contact ICC that complies with ISO/IEC 7816.

The area directly above zone 8 is also reserved space that could be used for the ICC. This is to accommodate the placement of the ICC by different card manufacturers.

Zone 8 – Employee Affiliation: Employee affiliation must be printed on the right side of the card. Employee affiliations will vary between Federal organizations. Some examples of employee affiliation are “Contractor,” “Active Duty,” “Civilian,” and “Foreign National.”

Zone 10 – Organizational Affiliation: The name of the Federal department or agency, or other organization, must be printed under the affiliation. The dimensions of this zone are 10.0 x 20.75 mm.

Zone 14 – Expiration Date: The card expiration date must be printed in YYYYmmdd format. The dimensions of this zone are 4.5 x 20.75 mm.

Federal Identity Management Handbook

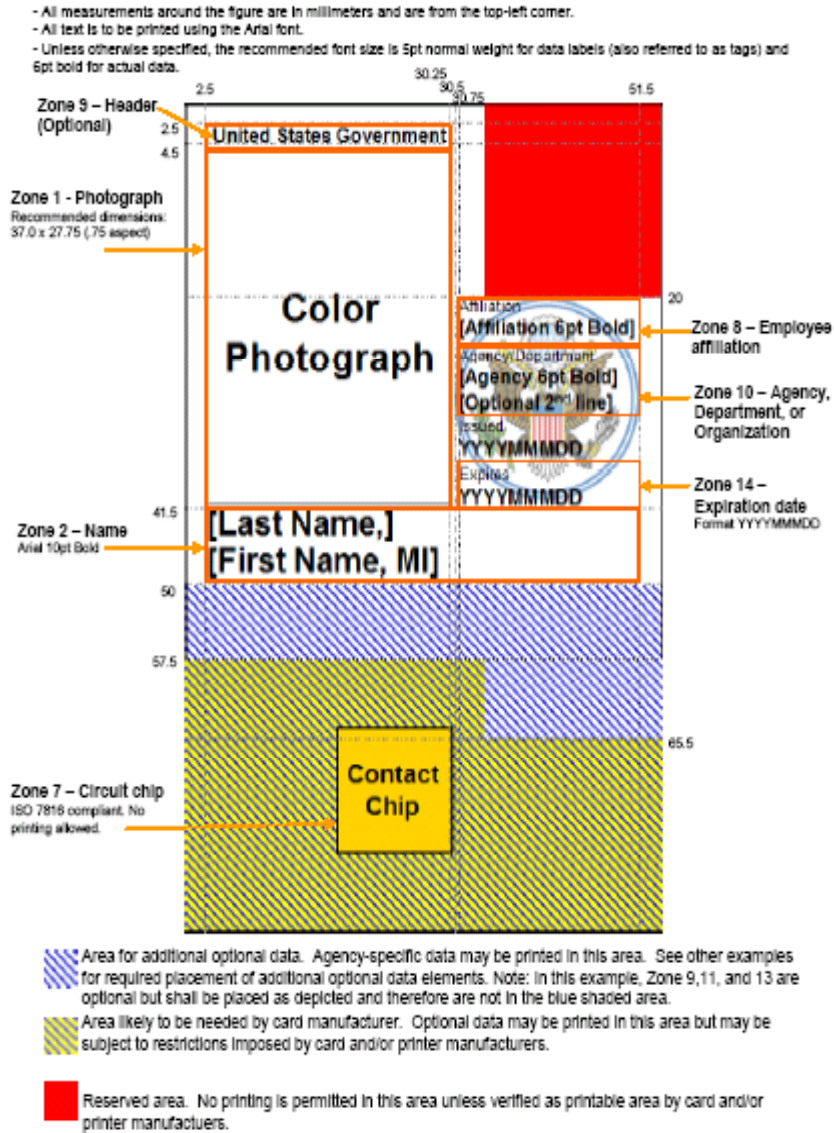


FIGURE 3. PIV CARD FRONT – PRINTABLE AREAS AND REQUIRED DATA¹²

¹² Ibid.

Federal Identity Management Handbook

4.1.1.1.2 *Back*¹³

Zone 1 – Agency card serial number: A unique serial number from the issuing department or agency must be printed on the card as shown in Figure 4.

The number can be formatted at the discretion of the issuing department or agency. Agencies will need to devise and promulgate their unique agency card serial numbers. Individual agencies should engage with their card manufacturers and decide at what point in the card issuance process the agency card serial number should be placed on the PIV card.

Zone 2 – Issuer identification: An issuer identification, consisting of 6 characters for the department code, 4 characters for the agency code, and a 5-digit number that uniquely identifies the issuing facility within the department or agency, must be printed on the card. Agency codes should be chosen so that they are in compliance with *FIPS 95-2, Codes for the Identification of Federal and Federally Assisted Organizations*. Individual agencies are responsible for selecting and implementing a numbering scheme that uniquely identifies each issuing agency within the agency.

¹³ Ibid.

Federal Identity Management Handbook

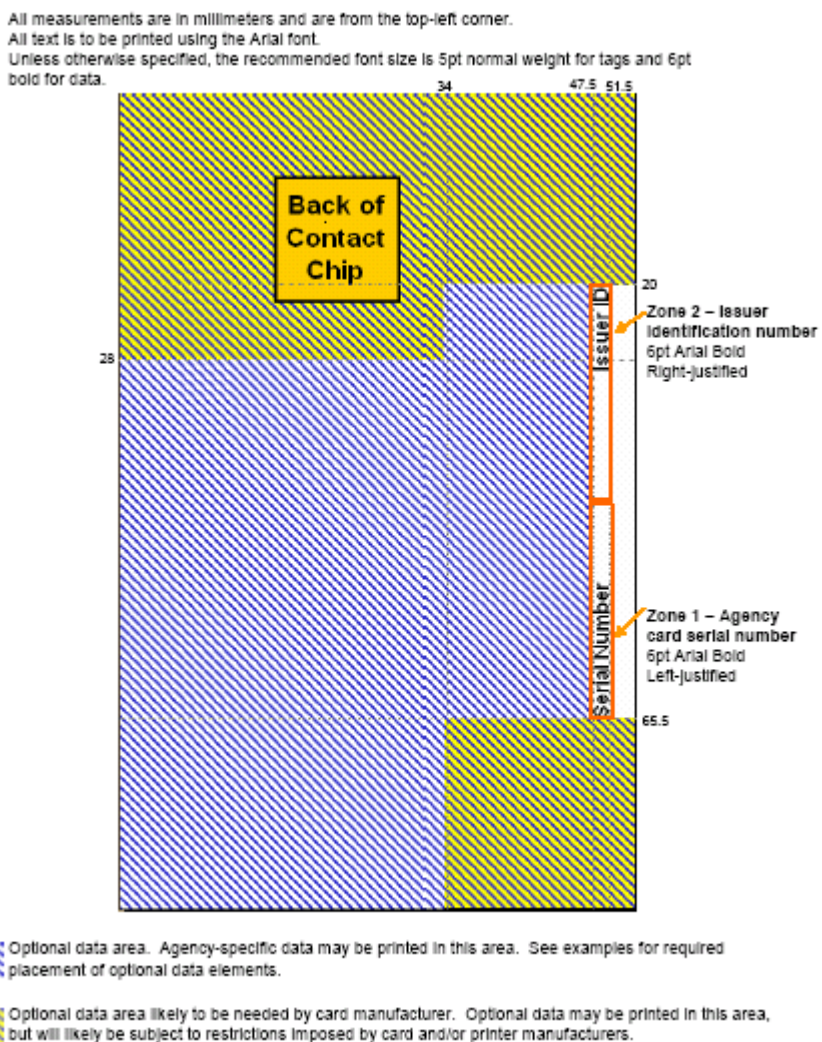


FIGURE 4. CARD BACK – PRINTABLE AREAS AND REQUIRED DATA¹⁴

¹⁴ Ibid.

4.1.1.2 Optional PIV Card Elements

Several optional data elements can be implemented on both the front and back of a PIV card. The placement and formatting of each optional visual element is illustrated in Figure 5, Figure 6, Figure 7 and Figure 8.

4.1.1.2.1 *Front*¹⁵

Zone 3 – Signature: If included, a signature it must be placed below the photograph and cardholder name. The space for the signature must not interfere with contact or contactless placement of the card. Because of space constraints, including a signature may limit the size of the optional two-dimensional bar code. The dimensions of this zone are 7.5 x 49.0 mm.

Zone 4 – Agency Specific Text Area: This area can be used at the discretion of individual agencies.

Zone 5 – Rank: If included, rank must be printed as shown in Figure 5. The rank can be formatted at the discretion of the department or agency.

Zone 6 –PDF two-dimensional bar code: If included, a PDF bar code it must be located on the left side of the card. If a cardholder’s signature is included (Zone 3), the size of the PDF bar code may be affected. The card issuer should confirm that a PDF bar code used in conjunction with a cardholder’s signature can satisfy the anticipated PDF data storage requirements.

Zone 9 – Header: If included, the text “United States Government” must be placed as shown in Figure 6. 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. The dimensions of this zone are 2.0 x 27.75 mm.

Zone 11 – Agency seal: If included, the agency seal should be printed as shown in Figure 5. To ensure that the information printed on the seal is legible and clearly visible, the seal should be printed according to the guidelines in Figure 5. The dimensions of this zone are 20.0 x 20.0 mm. Agencies may also print their seals in other locations if the seal does not interfere with any of the mandatory data elements or technologies on the card

Zone 12 – Footer: The footer is the preferred location for the Emergency Response Official Identification label, if included. A department or agency can print “Federal Emergency Response Official,” preferably in red. Departments and agencies can also print a second line in Zone 9 that further identifies the Federal emergency respondent’s official role. Some examples of official roles are “Law Enforcement, “Firefighter” and “Emergency Response Team (ERT).”

Zone 13 – Issue Date: If included, the issue date must be printed to the left of the expiration date in YYmmdd format.

Zone 15 – Color-Coding for Employee Affiliation: Color-coding can be used to further identify the employee’s affiliation. If included the color must be used as a background color for the information in Zone 2 (name), as illustrated in Figure 7. Blue, red, and green must be used as follows:

- Blue for foreign nationals

¹⁵ Ibid.

Federal Identity Management Handbook

- Red for emergency responder officials
- Green for contractors

Zone 15 can be solid or patterned, at the department's or agency's discretion. The dimensions of this zone are 8.5 x 49.0 mm.

Zone 16 – Photo Border for Employee Affiliation: A border can be used around the photograph to further identify the employee's affiliation, as illustrated in Figure 6. This border can be used in conjunction with color coding (Zone 15) to enable departments and agencies to identify various employee categories. The photo border cannot obscure the photo. The border can be a solid or patterned line. Blue, red, and green must be used as follows:

- Blue for foreign nationals
- Red for emergency responder officials
- Green for contractors

All other colors can be used at the department's or agency's discretion.

Zone 17 – Agency Specific Data: In cases in which other defined optional elements are not used, Zone 17 can be used for other department- or agency-specific information.

Federal Identity Management Handbook

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

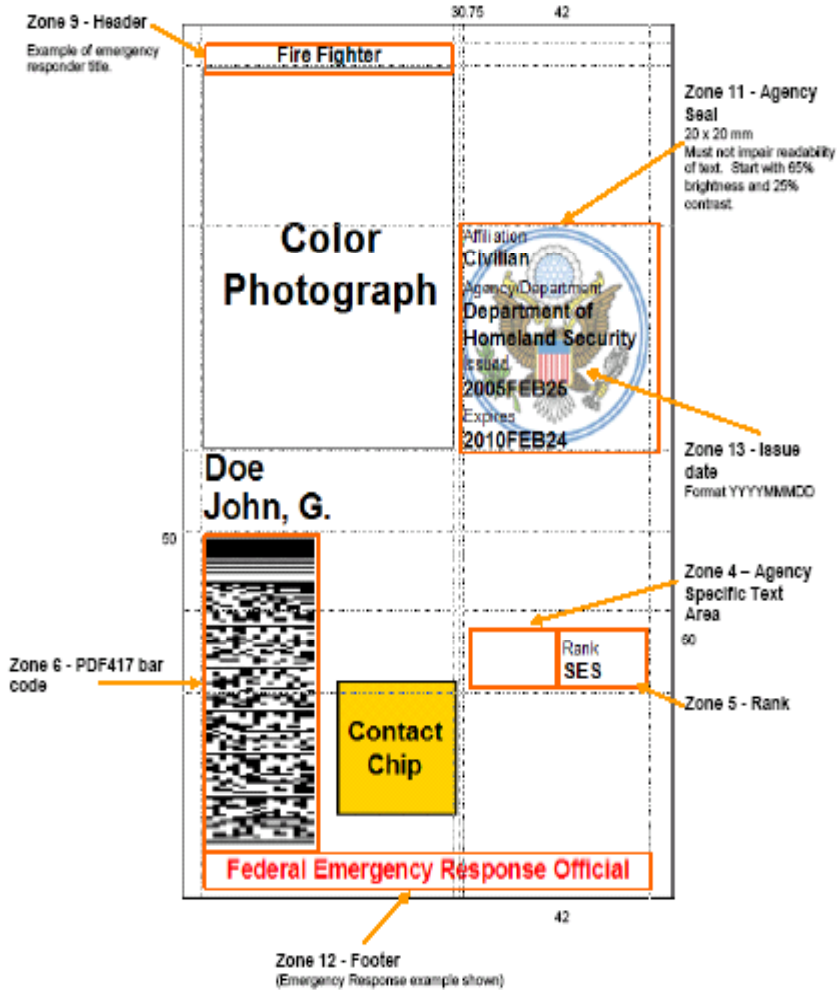


FIGURE 5. CARD FRONT – OPTIONAL DATA PLACEMENT – EXAMPLE 1¹⁶

¹⁶ Ibid.

Federal Identity Management Handbook

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

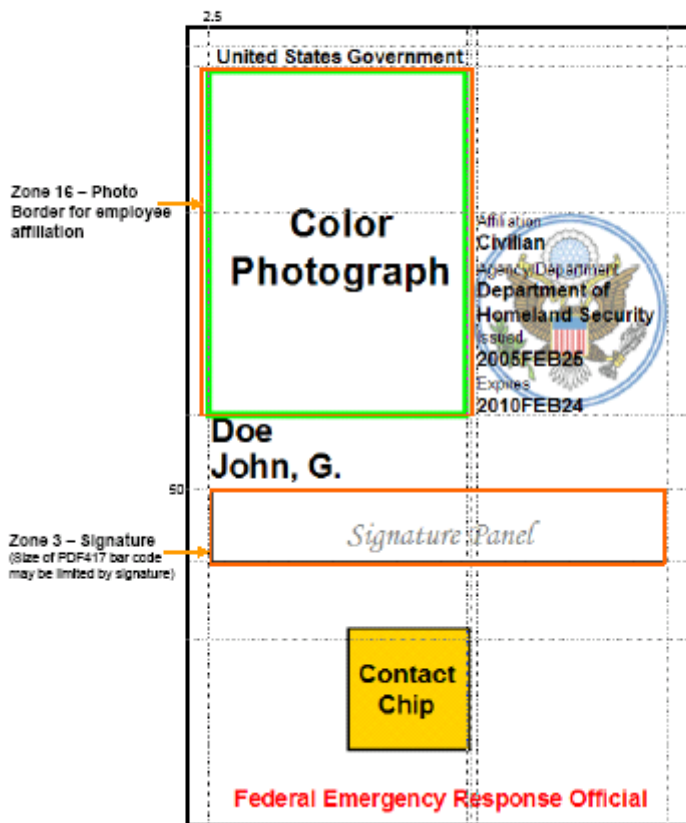


FIGURE 6. CARD FRONT – OPTIONAL DATA PLACEMENT – EXAMPLE 2¹⁷

¹⁷ Ibid.

Federal Identity Management Handbook

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

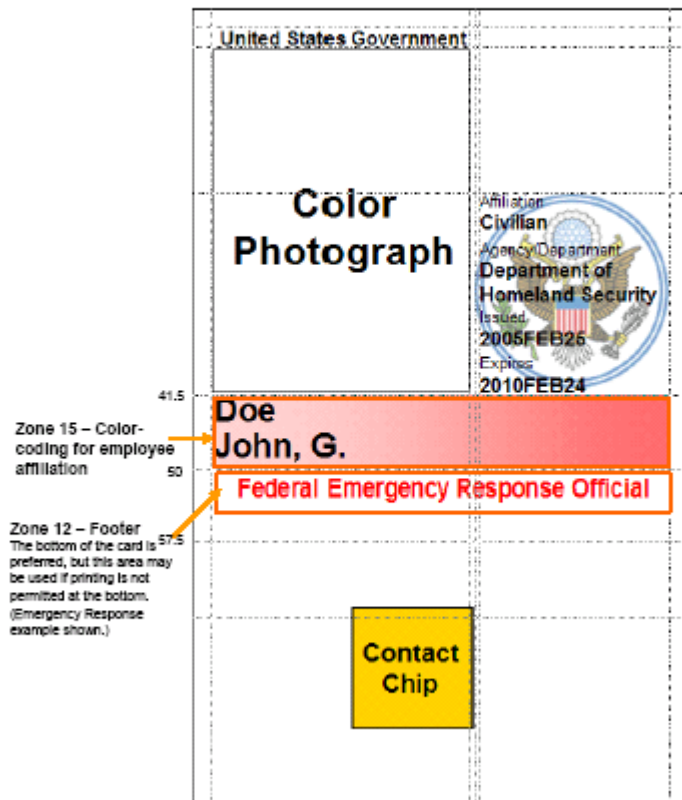


FIGURE 7 CARD FRONT – OPTIONAL DATA PLACEMENT – EXAMPLE 3¹⁸

¹⁸ Ibid.

Federal Identity Management Handbook

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

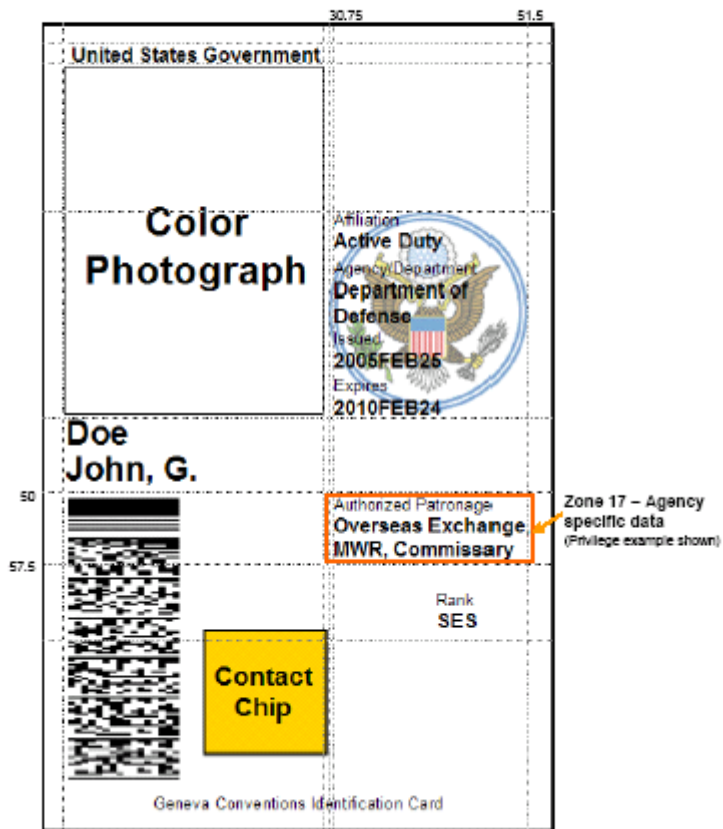


FIGURE 8. CARD FRONT – OPTIONAL DATA PLACEMENT – EXAMPLE 4¹⁹

¹⁹ Ibid.

4.1.1.2.2 *Back*²⁰

Zone 3 – Magnetic Stripe: If included, a magnetic stripe must have high coercivity and be placed according to the standards in ISO/IEC 7811.

Zone 4 – Return To: If included, return to information must be placed on the back of the card. Generally, the language is “If Found Return to:” and an address. In general agencies should place the language as depicted in Figure 9.

Zone 5 – Physical Characteristics of Cardholder: If the cardholder’s physical characteristics (e.g., height, eye color, hair color) are included, they must be printed in the general area identified in Figure 9.

Zone 6 – Additional Language for Emergency Responder Officials: Departments and agencies may choose to provide additional information to identify emergency response officials or to identify the cardholder’s authorized access better. Such additional text may be printed in the general area identified in Figure 9 and should not interfere with other printed text or machine-readable components. Individual agencies will have specific guidance concerning the text that is acceptable for Zone 6. Although, example language could include the following: “First Responder” or “Federal Emergency Response Official.” Example language is also provided in Figure 9.

Zone 7 – Standard Section 499, Title 18 Language: If standard Section 499, Title 18 language warning against counterfeiting, altering, or misusing the card is used, it must be printed in the general area identified in Figure 9. Section 499, Title 18 specifically states the following (agencies can chose to paraphrase): “Whoever falsely makes, forges, counterfeits, alters, or tampers with any naval, military, or official pass or permit, issued by or under the authority of the United States, or with intent to defraud uses or possesses any such pass or permit, or personates or falsely represents himself to be or not to be a person to whom such pass or permit has been duly issued, or willfully allows any other person to have or use any such pass or permit, issued for his use alone, shall be fined under this title or imprisoned not more than five years, or both.”²¹

Zone 8 – Linear 3 of 9 Bar Code: If included, a bar code must be placed as illustrated in Figure 9. The bar code must conform to the standards set by the Association for Automatic Identification and Mobility (AIM). The beginning and end points of the bar code will depend on which contactless module is embedded. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.

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

Zone 10 – Agency-Specific Text: Like Zone 9, Zone 10 can be used to provide department- or agency-specific information.

Figure 9 and Figure 10 illustrate the placement of optional data on the back of a PIV card as depicted in FIPS 201.

²⁰ Ibid.

²¹ Title 18, United States Code Section 499, Military, Naval, or Official Passes, January 6, 2003.

Federal Identity Management Handbook

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 8pt normal weight for tags and 6pt bold for data.

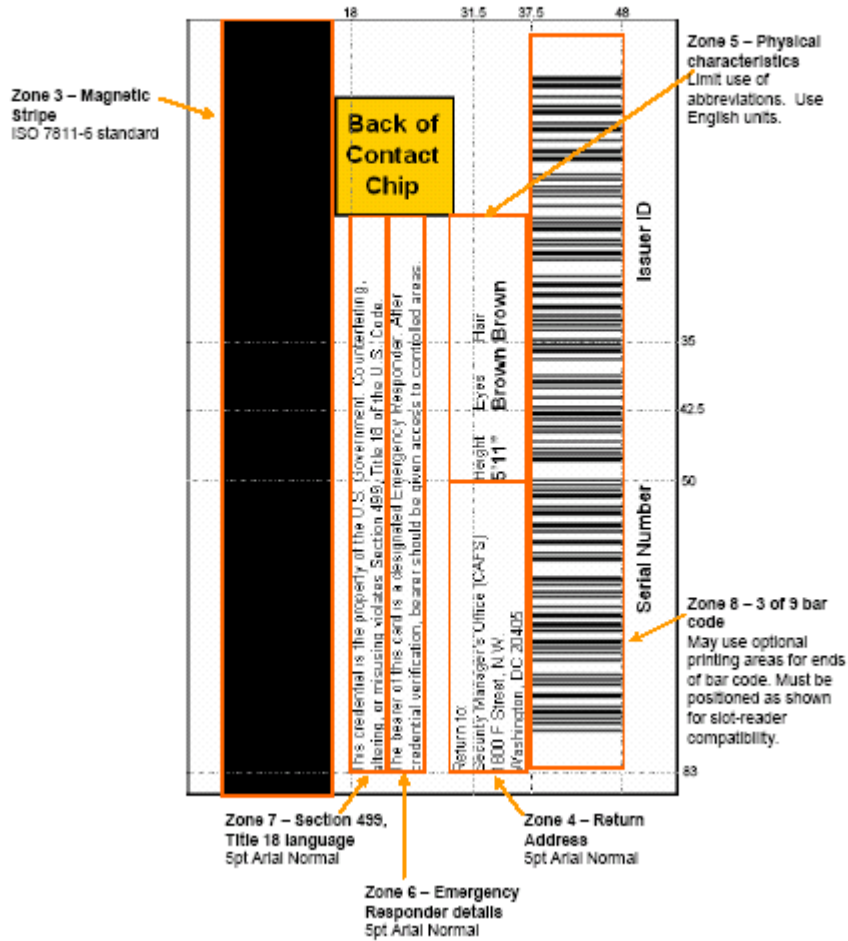


FIGURE 9. CARD BACK – OPTIONAL DATA PLACEMENT – EXAMPLE 1²²

²² Ibid.

Federal Identity Management Handbook

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.

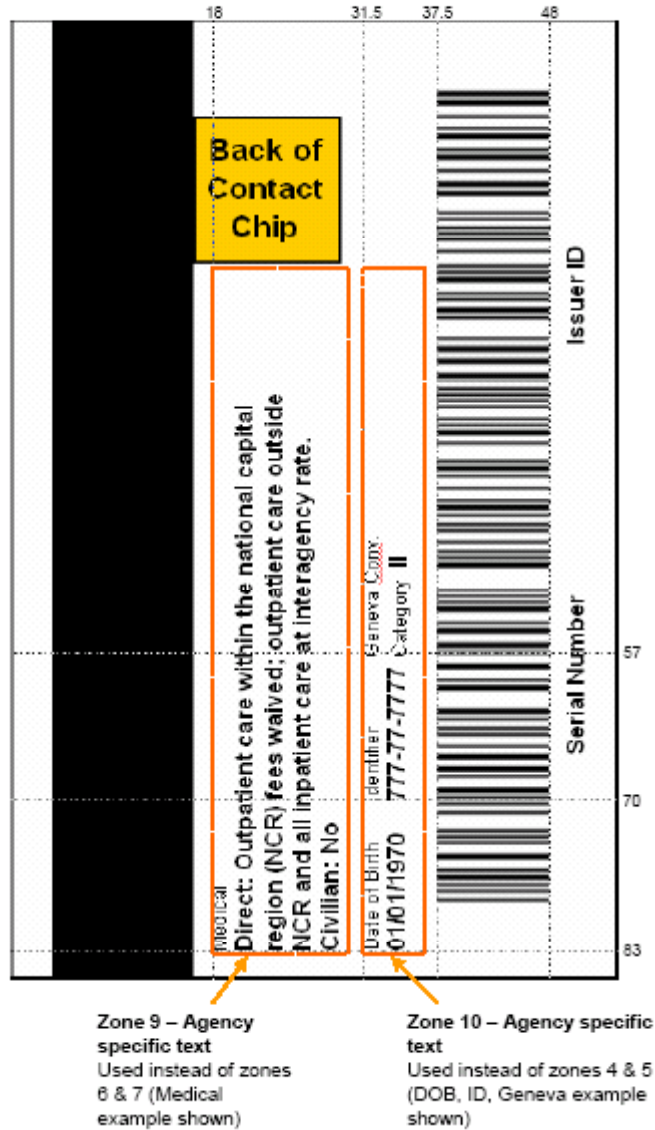


FIGURE 10. CARD BACK – OPTIONAL DATA PLACEMENT – EXAMPLE 2²³

²³ Ibid.

4.1.2 Implementation Recommendations

The following section provides recommendations for agencies to follow for implementation of FIPS 201 card specifications. Regardless of which methods are selected, however, the card must comply with the FIPS 201 physical specifications.

4.1.2.1 Card Printing

FIPS 201 levies two requirements concerning the printed material of a PIV card. The printed information on a PIV card should not rub off during the life of the card. Additionally, the printing process should not deposit debris on the printer rollers during printing and lamination of the card.²⁴

An agency can choose from several commonly accepted printing methods to personalize PIV cards. Such methods include standard dye-sublimation printing, reverse dye printing, thermal transfer printing, and laser etching. The printing method selected will determine the quality and durability of the end product. Tradeoffs can include production costs and levels of maintenance and support. Various vendors offer different models of printers. ID card printers can vary in cost, quality, and capability. (For more information on card printers and consumables see Section 4.8.)

It is estimated that, with normal usage, the useful life of a new PIV identification card is 3–5 years. FIPS 201 requires the PIV card to be valid for no more than 5 years.²⁵ Every card will experience normal wear and tear associated with usage. It is to be expected that a certain percentage of cards will need to be replaced before their normal end-of-life (EOL). Additionally, PIV cardholders will use their cards with different frequencies, and the more frequently a PIV card is used, the more likely it is to wear out. Agencies will want to inform and educate PIV cardholders on the proper use and storage procedures for their PIV cards. This will reduce replacement costs due to re-issuance of cards before their EOL.

Regardless of the printing method and printer model used, PIV credential printers should receive regularly scheduled maintenance to ensure that the printers are working properly and that debris is cleaned from the printer rollers. Also, agencies should follow manufacturer recommendations for printer maintenance. This will help ensure proper printing of PIV cards and also reduce the number of defective cards produced. Proper training should be provided to those individuals who are responsible for printer maintenance to ensure that they are aware of the proper procedures for cleaning card printers.

4.1.2.2 Tamper-Resistant Security Features

Federal agencies must incorporate at least one tamper-proofing and resistance security feature into their PIV cards. Tamper-resistant security features for the purposes of this document are defined as features that are incorporated into the card body to reduce counterfeiting, resist tampering, and provide visual evidence of attempts to tamper with a PIV card. Tamper-resistant security features can be incorporated into the PIV card either by printing or incorporation into the card laminate. Agencies are strongly encouraged to review their requirements and incorporate commensurate security features to the

²⁴ Ibid.

²⁵ Ibid.

Federal Identity Management Handbook

maximum extent practicable and cost effective in order to reduce the risk of a PIV card being tampered with or illegally duplicated.

One security feature commonly implemented on identity cards is a hologram. Holograms are either generic, meaning that the image is non-specific and therefore available to the general public, or customized, meaning that the image is of something specific such as a corporate or agency logo. Custom holographic images are often registered or trademarked to prevent unauthorized use. Holograms that are customized can be more expensive to produce, and the lead times for graphic design may be longer; however, such holograms can provide a greater level of security than generic holograms. Other examples of security features that can be included on the card body include:

- Optical varying structures
- Optical varying inks
- Holographic images (ghost images)
- Hidden text
- Water marks
- Laser etching and engraving

All tamper-resistant and anticounterfeiting methods implemented by agencies must meet the following requirements:

- The security features are implemented in accordance with durability requirements specified in ISO/IEC 7810.
- The security features are free from defects.
- The security features do not obscure printed information on the PIV card.
- The security features do not impede access to machine-readable information on the PIV card.

Agencies should work closely with their card vendors and systems integrators to evaluate which security methods are most suitable. Agencies may also want to consider a combination of security features to achieve a higher confidence that the PIV card is tamper resistant.

4.1.2.3 Physical Characteristics and Card Durability

PIV credentials must adhere to multiple commonly accepted smart-card specifications. These specifications are identified in Section 4.1.3 of FIPS 201. They include:

- ISO/IEC 7810
- ANSI 322
- ISO/IEC 10373

The standards and specifications can be found in their entirety and are available for a fee from the ISO web site (www.iso.org). FIPS 201 levies additional requirements:

1. PIV cards must contain both a contact and a contactless interface.

Federal Identity Management Handbook

2. Agencies may elect to punch a hole in the PIV card body to enable the card to be worn on a lanyard.
3. The PIV card shall not be embossed.
4. Decals shall not be stuck to the card.

The FIPS 201 specification does not prescribe whether the required contact and contactless interface for a PIV card should be implemented as a dual-interface or a hybrid smart card. Therefore, each agency can evaluate which type of smart card to implement. Dual-interface smart cards contain a single chip capable of conducting both contact and contactless transactions. Hybrid cards contain both a contact chip and a contactless chip. The two chips are not connected and perform their contact and contactless functions independently.

Agencies should be cautious when deciding whether to punch holes in their PIV cards. They should ensure that planned alterations are coordinated with the card manufacturer and do not affect card performance, durability, or the information visible on the PIV card.²⁶ Strict guidelines must be associated with the practice of punching holes in PIV cards, and the practice should be monitored closely by agencies implementing it. Plastic ID cardholders into which an ID card can be inserted are commonly available, for use with a lanyard. This method does not require punching a hole in the PIV card.

4.1.2.4 Topology

In addition to the mandatory data elements, a card can include certain optional data elements that agencies may find useful. The optional elements allow individual agencies to tailor their PIV credentials to meet their specific needs and provide additional security features. For example, optional PIV elements that can provide additional levels of assurance include the signature of the PIV cardholder, color coding for employee affiliation, and physical characteristics (i.e., height, weight, eye color, hair color) of the PIV cardholder. Individual agencies may find it useful to identify what items are included on their current identity credentials and what items are currently recognizable to security personnel. Agencies can then decide what optional topology elements to implement. While each additional item placed on a card may make it more difficult for the card to be replicated illegally, agencies should note that card topology management also becomes more complex with each additional item placed on the card.

In addition to the mandated technologies, agencies may have to accommodate certain technologies to support legacy applications. These technologies include bar code and magnetic stripe technologies. The types of bar codes supported by FIPS 201 include a PDF 417 two-dimensional bar code and a linear 3 of 9 bar code, as defined by AIM standards. The magnetic stripe must have high coercivity and its placement must conform to ISO/IEC 7811. Whenever possible, use of these technologies should be limited in favor of the more secure ICC technology that is included on all FIPS 201 compliant PIV cards.

The specific requirements for placement and format of data elements on a PIV card are included in Figure 3 through Figure 10 and in Section 4.1 of FIPS 201.

²⁶ Ibid.

4.1.3 PIV Logical Data

Logical information refers to the data that is stored in the PIV card ICC. The mandatory logical data elements are as follows:

- A personal identification number (PIN), used to prove the identity of the cardholder to the card (CTC authentication)
- A cardholder unique identifier object (CHUID), used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system
- A PIV authentication data (one asymmetric key pair and corresponding certificate associated with the cardholder), used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system
- Two biometric fingerprints, used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system and used if agencies choose to implement on-card matching of biometric information

Table 4 summarizes the mandatory logical data elements stored on a PIV card and their authentication categories.

Table 4. PIV Card Mandatory Logical Elements and Categories of Use

Data	Use
PIN	Cardholder to card (CTC)
CHUID	Cardholder to external entity (CTE)
PIV Authentication data	Cardholder to external entity (CTE)
Two biometric fingerprints	Cardholder to external entity (CTE)

Several optional data elements can also be stored in the PIV card ICC. The FIPS 201 standard establishes requirements for these logical elements. These elements include:

- Asymmetric key pair and corresponding certificate for:
 - Digital signatures, used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system
 - Key management, used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system
- Asymmetric or symmetric local authentication keys for supporting additional physical access specifications, used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system
- Symmetric keys for card management system, used by the card to prove the identity of the cardholder to an external entity (CTE authentication), such as a network computer system

Table 5 summarizes the optional logical data elements stored on a PIV card and their authentication categories.

Table 5. Optional Logical Elements and Categories of Use

Data	Use
Asymmetric key pair - digital signature	Cardholder to external entity (CTE)
Asymmetric key pair - key management	Cardholder to external entity (CTE)
Asymmetric or symmetric keys - local authentication	Cardholder to external entity (CTE)
Symmetric key(s) - card management system	Cardholder to external entity (CTE)

It is important to note that the only biometric data that is required to be stored on the PIV card are two electronic fingerprints. There is no requirement to store the applicant’s electronic facial image on the PIV card. The electronic facial image is stored in a database maintained by the PIV Registrar, and its use is mandatory only under certain circumstances. The specific requirements for biometric data and uses are described in Section 4.4.

The logical data structure of a PIV card supports both multi-programmable and file system card platforms. The logical data structure provides the exact data elements, their format, and where to locate them on the chip. SP 800-73 provides the technical specifications for an interoperable PIV card, including cryptographic keys and other authentication objects.

4.1.3.1 Activation of a PIV Card

In order to perform the biometric and asymmetric authentication described above, the PIV card must be activated. This is because reading the biometric information on the card and using the asymmetric keys are considered privileged operations.²⁷ When cardholder activation is required, the activation must be PIN based. For example, an agency may want to implement a fingerprint biometric check at a physical access point. The PIV cardholder will be asked to enter a PIN at the physical access point. The PIN is transmitted to the PIV card and checked by the card. If the PIN is correct, the card is activated and the biometric can be read.

PIV cards can also be activated by the card management system, for card personalization or post-issuance card updates. Card personalization or updates must be performed using a challenge-response protocol as specified by SP 800-73. During card personalization, card management keys must be unique for each PIV card, meaning that one cryptographic key cannot be used to activate more than one card.

4.1.3.2 CHUID

The CHUID is a container²⁸ and a mandatory data element. The CHUID container includes the FASC-N. The FASC-N uniquely identifies each PIV credential. The CHUID is a free read data element from both the contact and contactless interfaces (the PIV card doesn’t have to be activated for an electronic

²⁷ Ibid.

²⁸ A container is a concept that was introduced by the Government Smart Card Interoperability Specification document. Container refers to the concept of placing data elements that have the same access control rules in one standard location, hence the term container. Additionally, a container generally has a group of data elements that are accessed at the same time.

reader to read the CHUID). The format of the CHUID is specified in *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems v2.2*, commonly referred to as PACS v2.2.

FIPS 201 requires two additional unique data elements in the CHUID container. The first is an expiration date, which facilitates status checking in the asymmetric signature field. The second is the format of the asymmetric signature field is specified in FIPS 201. For additional information about the CHUID, see Section 4.2 of FIPS 201 and SP 800-73.

4.1.4 Communication with the User Community

After agencies select and implement the physical, visual, and logical elements that will be placed on their PIV cards, they should communicate with their user community and educate them on the visual, physical, and logical specifications of their PIV cards. This communication is essential in gaining the acceptance of users and ensuring a smooth transition to a fully compliant PIV card. If users are aware of what the credential looks like, what its functionality is, what information is stored on the card, and how the information will be used, they will be more likely to accept the PIV card.

To accomplish this, agencies may find it useful to provide intra-agency marketing materials to their user communities. More information on stakeholder involvement in the PIV program can be found in 5.2. Some materials that agencies may want to consider developing are:

- Informational briefings
- Pamphlets
- User symposiums
- Direct e-mail messages

4.2 Logical Access Control

4.2.1 PIV Card Cryptographic Specifications

The FIPS 201 cryptographic specifications provide Federal agencies and PKI vendors with a clear definition of the algorithms and key management processes that must be used in conjunction with PIV cards for access control applications. The FIPS 201 cryptographic specifications enable agencies and their PIV cardholders to exchange electronic data in a process that is supported by the principles of integrity, confidentiality, non-repudiation, and secure authentication. The use of cryptographic mechanisms in conjunction with the PIV card increases the assurance that the cardholder's demographic data is bound to the card and that the cardholder can send and receive electronic data securely.

Cryptographic Requirements

One function of the PIV card is to authenticate the card itself to a back-end system. Such authentication is essential to ensure that the card being presented is a valid PIV card that was issued in compliance with FIPS 201. To meet this objective, the FIPS 201 cryptographic specifications identify a single mandatory key that must be stored on the card. This key, the PIV authentication key, is an asymmetric private key that enables the cardholder to access physical and logical access-control applications.

Asymmetric key cryptography uses a secure public and private key pair to encrypt and decrypt messages.

To enable key cryptography, the PIV card must implement the following functions²⁹:

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

4.2.2 Cryptographic Implementation Guidance

FIPS 201 specifies four optional keys that agencies can use in addition to the mandatory authentication key. Use of the optional keys will be contingent upon each agency's cryptographic requirements. Of course, it is likely that an agency may require many different combinations of optional keys, given the diversified needs of users. The optional keys are as follows:

- **Card authentication key.** This key can be either an asymmetric or symmetric private key and is used exclusively for physical access control.
- **Digital signature key.** This key is an asymmetric private key used for signing documents.
- **Key management key.** This key is an asymmetric private key used for key establishment and transport.
- **Card management key.** This key is a symmetric key used for card personalization and in post-issuance card lifecycle processes.

An agency's cryptographic requirement will determine which optional keys it uses. An agency with diversified user needs may require cards carrying different combinations of optional keys.

FIPS 201 establishes three levels of assurance to provide agencies with a choice for accommodating different security needs. For further guidance, refer to Section 4.7.

4.2.2.1 Cryptographic Algorithms

FIPS 201 requires agencies to select one of two certified cryptographic encryption algorithms. These algorithms are commercially available, and the PIV card has enough allocated storage space for the keys. Over time, the keys will be migrated to more advanced encryption algorithms. Table 6 lists the algorithm associated with each key type, the key sizes, and the certificate expiration dates.

²⁹ FIPS PUB 201, op. cit.

Table 6. PIV Key Types³⁰

Key Type	Certificate Expiration Date	Algorithm and Key Size (bits)
Authentication	Present - 12/31/2010	RSA 1024 or ECDSA 160
	12/31/2010 -	RSA 2048 or ECDSA 224
Local authentication	Present - 12/31/2010	Two Key Triple - DES Three Key Triple - DES AES-128, AES-192, and AES-256 RSA 1024 ECDSA 160
	12/31/2010 -	Three Key Triple - DES AES-128, AES-192, and AES-256 RSA 2048 ECDSA 224
Digital signature	Present - 12/31/2007	RSA 1024 or ECDSA 160
	12/31/2007 -	RSA 2048 or ECDSA 224
Key management	Present - 12/31/2007	RSA 1024 or ECDSA 160
	12/31/2007 -	RSA 2048 or ECDSA 224
Card management	Present - 12/31/2010	Two Key Triple - DES Three Key Triple - DES AES-128, AES-192, and AES-256
	12/31/2010 -	Three Key Triple - DES AES-128, AES-192, and AES-256

4.3 Physical Access Control

It would be difficult to recall a time when agencies of the Federal Government operated without a physical access control system (PACS) based on a credential that allows people both to communicate with the system and access Federal buildings. PACSs have many benefits, foremost among which are their use of mature and proven technologies that can strengthen the trust relationship between an agency and an employee and enhance the level of security with which employees interact with building facilities.

Substantial guidance is available to agencies considering the deployment of a new PACS or upgrading a current system. The widespread use of PACSs and the presence of a mature marketplace offer agencies the advantage of steadily declining prices for physical security products. Both factors have also contributed to the widespread adoption of PACSs by Federal agencies.

Currently, there are a variety of autonomous PACSs at the Federal level. Agencies originally deployed a PACS according to their local security requirements, leading to the adoption of numerous incompatible systems. Such systems cannot share information readily or authenticate employees from different agencies.

³⁰ NIST Special Publication 800-78, *Recommendation for Cryptographic Algorithms and Key Sizes*, NIST, February 2005.

Federal Identity Management Handbook

Recently, the Federal Government has taken a more proactive role by initiating substantial changes to agency PACS policies. Significant progress has been made through the development and adoption of GSA's Government Smart Card Interoperability Specification (GSC-IS). The GSC-IS defines an architectural model for interoperable smart cards. FIPS 201 has also advanced the goal of a standardized and interoperable system for physical access.

4.3.1 Physical Access Control System Components

A PACS that is based on smart cards is composed of the following components:

- **PIV Card.** The PIV card stores a cardholder's access control information. It is presented to a card reader to enable an authentication transaction.
- **PIV Card Reader.** The card reader provides power to the card's interface and extracts the cardholder's information from the card. It then sends the information to the control panel. Although it is less common to use the contact interface for physical access, one can do so by inserting the card directly into the reader.
- **Control Panel.** The control panel receives the user's information from the card reader and either makes an access control decision or forwards the cardholder's information to an access control server for a decision.
- **Access Control Server.** The access control server renders an access decision based on the information submitted by the control panel and the user's information in the cardholder data repository.
- **PIV Cardholder Data Repository.** The cardholder data repository manages PIV cardholder access control privileges.
- **Door Lock.** The door lock receives a signal from the control panel to unlock the door or inform the PIV cardholder that access has been denied.

The access control transaction should appear seamless to the PIV cardholder. To make this possible, various components work together to authenticate cardholders at levels consistent with agency security requirements and at transaction speeds that are acceptable to the cardholders. Figure 11 illustrates the process.

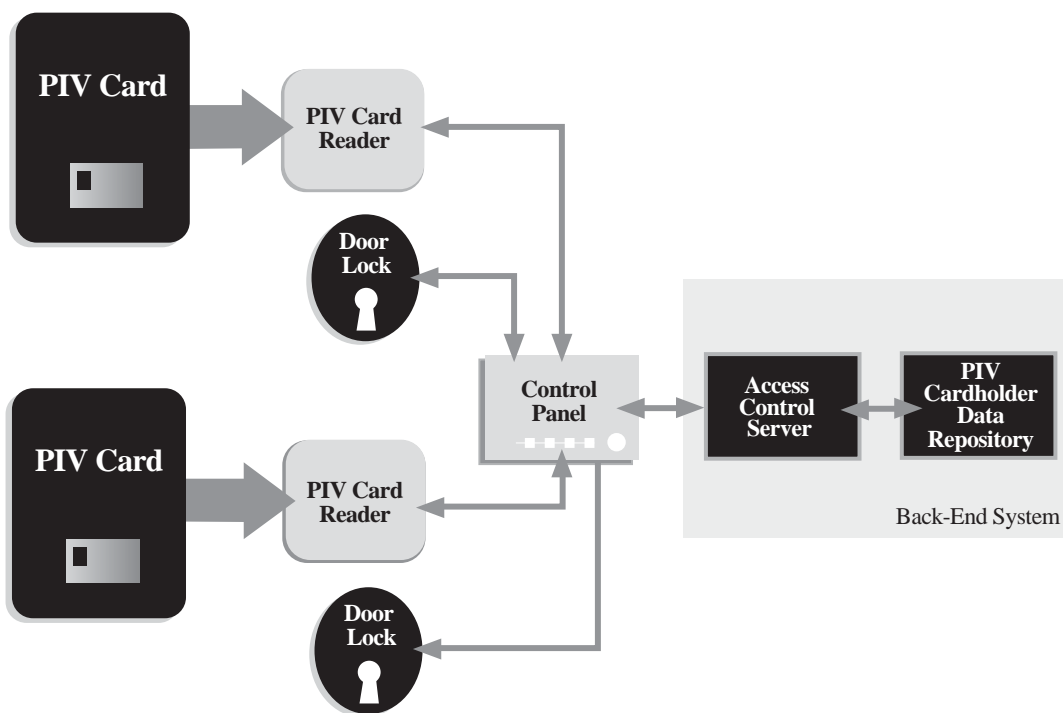


FIGURE 11. PHYSICAL ACCESS CONTROL SYSTEM

4.3.2 Physical Access Interoperability Guidelines

FIPS 201 does not mandate specific PACS mechanisms. Instead, the standard references a document published by the Physical Access Interagency Interoperability Working Group (PAIIWG), which helps agencies understand the technical components of a PACS and provides guidance for implementing a minimum level of security and interoperability between a smart card and a reader. Agencies should reference this document when designing a PACS.

4.3.2.1 Physical Access Interagency Interoperability Working Group

The PAIIWG is a government and industry partnership created to provide smart card physical access interoperability solutions to the Federal Government.

The PAIIWG's official mission focuses on the following goals³¹:

- Create a physical access interoperability guidance document for use by Federal departments and agencies, to include the following technical specifications:
 - A new credential numbering system to augment the SEIWG-012
 - A method for providing a secure form of card authentication
 - A means of protecting the card PIN when used

³¹ Federal PKI Deployment Workshop 2: Federal Credential And Beyond, presentation by Mike Sulak, May 12, 2004.

Federal Identity Management Handbook

- A discussion of contact and contactless interoperability issues
- Promote industry membership in the PAIIWG.
- Encourage industry participation in developing technical standards and guidelines.
- Develop government and industry consensus on a technical framework.
- Submit the technical guidance to the IAB for final approval and submission to the FICC.

4.3.2.2 Technical Implementation Guidelines

The solutions developed by the PAIIWG are incorporated in a document called the *Technical Implementation Guidance (TIG): Smart Card Enabled Physical Access Control Systems Version 2.2*. The TIG is not a standard that requires agency compliance. The objective of the TIG is to define specifications to enable agencies to procure and implement hardware and software for PACSs such that these systems will achieve the following goals:

1. Operate with the Federal Agency Smart Credential (FASC).
2. Facilitate cross-agency Federal enterprise interoperability.
3. Allow a legacy PACS to operate with FASC-compatible card readers until the system is upgraded.

4.3.2.3 Card Specifications

The centerpiece of the TIG is the FASC-N, a unique number assigned to one individual. This number will be associated with the individual as long as that person is employed by the issuing agency. A new FASC-N will be assigned if the individual transfers to a different agency.

The FASC-N supports a centralized numbering scheme that is designed to limit nonrepudiation and reciprocity of Federally issued credentials. While the agencies themselves continue to be responsible for issuing credentials to employees and creating FASC-Ns, the TIG provides the government with a standardized credential for physical access control applications. FIPS 201 mandates that a FASC-N be created for each PIV card applicant and stored on the PIV card.

4.3.2.3.1 Card Holder Unique Identifier

The CHUID is a data file that is unique for each cardholder. The CHUID establishes a standardized data model for Federal agencies to use in their PACS applications. It provides detailed guidance regarding the configuration of data model components according to their data elements, tags, types, and maximum byte sizes. The CHUID container is an elementary file that is a required part of the data model for all PIV cards.

4.3.2.3.2 Federal Agency Smart Credential Number

The FASC-N must always be present in the CHUID elementary file. This requirement enables agencies to create unique credential numbers for employees that will not be duplicated by other agencies as long as they comply with FIPS 201.

Federal Identity Management Handbook

There are billions of possible statistical permutations that an agency can achieve when it creates credential numbers. Agencies can select up to a maximum of 40 characters to compose the data stored on the FASC-N. Many agencies choose to combine the 4-digit System Code with the 6-digit Credential Number or simply use the employee's social security number (SSN). The TIG strongly discourages the use of SSNs because of the risk to individuals as a result of unauthorized disclosure. The SSN was a central data element of the SEIWG-012, the predecessor to the FASC-N.

To achieve full Federal interoperability of a PACS, agencies must at a minimum be able to distinguish 14 unique digits when matching FASC-N-based credentials to unexpired cardholders. This minimum threshold has been established to guarantee the uniqueness of all FASC-N cards.

4.3.2.4 Assurance Profiles

Federal agencies are responsible for authenticating the identities of employees, contractors, and other authorized personnel to whom they issue credentials. Once a chain of trust is established between the agency and its cardholders, the agency selects an assurance profile that will be compatible with its security needs.

The transaction between a PIV card and card reader can be more or less reliable, and an agency may have varying requirements for transaction reliability. These may reflect the value of the assets that a PACS is protecting. For this reason, FIPS 201 defines a range of assurance profiles—Some Confidence, High Confidence, and Very High Confidence—and associates each profile with an extensible data model based on PIV cards. Each profile correlates to a degree of confidence in the integrity of the transaction between the card and the reader. By using the methods prescribed for each assurance profile, a PACS can operate at the level of integrity and security required by the specific environment and facilitates cross-agency interoperability for the population of PIV cardholders. For a detailed process flow analysis of the various PIV card authentication mechanisms available to agencies, refer to Section 4.7.

4.3.2.5 Card Issuance Controls

The TIG does not address technical controls on the card issuance process. However, it is clear that controls are required on card personalization and the use of data from PIV cards. The issuer must control instantiation and modification of data on a PIV card, and individuals may control when data is released during use to prevent unintended or unauthorized disclosure of personal information. The PIV card technical controls are based on issuer-managed keys that must be protected. Issuer information systems must create and maintain card-unique keys such that no two cards have the same keys. The card-unique key may be implemented through key diversification, in which a master key and card data, such as a serial number, are combined in a cryptographic operation to produce card unique keys. In this case, the diversification master key must be maintained in a FIPS 140 Level 3 security device to ensure that a single compromise will not result in a loss of all PIV cards from a given issuer.

Summary

The publication of FIPS 201 and the TIG is bringing a new degree of compatibility and interoperability to the Federal identity management process. Until recently, agencies did not have access to specific guidance from a central authority that could facilitate the issuance of their credentials for physical access applications. Now, a data model has been introduced, based on the PIV card. The data model

supports a government-wide numbering scheme that also enables agencies to issue unique credentials. Agencies can follow the instructions presented in the TIG to achieve a standardized credential that is interoperable across the Federal enterprise.

4.4 Biometric Data Specifications

4.4.1 Use of Biometric Technologies

The use of biometric technologies has attracted significant attention in recent years as a strong authentication mechanism for access control applications. The ability to bind a cardholder’s physiological traits to a PIV card makes a convincing argument for using biometrics as a supplement or alternative to other authentication technologies. While biometrics can be used in almost any access control application, they typically are used as a secondary or tertiary form of authentication.

Although using biometric data as a strong authentication factor is considered acceptable, there are few actual use-case scenarios to help agencies determine how to use biometrics to achieve a target security level. This section documents the biometric technologies required by FIPS 201, evaluates the strengths and weaknesses of these technologies, and provides practical guidance for using these technologies at a Federal agency.

4.4.2 Biometric Data Requirements

Table 7 summarizes the FIPS 201 requirements for using biometric data.

Table 7. FIPS 201 Biometric Data Requirements

Data Type	Capture Format	Number	Use
Fingerprint	Image	10	Forensics/background check
Fingerprint	Image	2	Access control
Face	Image	1	Access control

FIPS 201 mandates the electronic capture of fingerprints and a facial image during the PIV identity-proofing process. Whenever possible, all 10 fingerprints must be collected so that a background check can be conducted. The selection of the fingerprint instead of a different biometric is partly based on the fingerprint being the de facto standard in forensic applications such as background checks. The FBI has established a database of millions of fingerprints that agencies will be able to query.

To meet the fingerprint requirement, agencies will have to procure a fingerprint acquisition device that complies with Appendix F of the FBI’s Electronic Fingerprint Transmission Specification,³² the BIOAPI,³³ and the CBEFF³⁴ standards. The captured images must be formatted according to the standards in INCITS 381-2004³⁵ and embedded within the CBEFF³⁶ data structure.

³² *Electronic Fingerprint Transmission Specification*, Federal Bureau of Investigation, Department of Justice, January 1999.

³³ INCITS 358-2002, *American National Standard for Information Technology—The BioAPI Specification*.

³⁴ NISTIR 6529-A—*Common Biometric Exchange Formats Frameworks*, NIST Interagency Report, April, 2004.

³⁵ INCITS 381-2004, *American National Standard for Information Technology—Finger Image-Based Data Interchange Format*.

³⁶ NISTIR 6529-A—*Common Biometric Exchange Formats Frameworks*, NIST Interagency Report, April, 2004.

Federal Identity Management Handbook

After they are acquired, fingerprint and facial images will be securely stored and maintained on a database server. Although a facial image of the PIV cardholder must be captured, this process does not require the use of a facial biometric system (i.e., a system that uses the image captured to automatically identify the PIV cardholder). Instead, an agency may use a digital camera to photograph the cardholder and print the facial image to the PIV card. While facial image acquisition can be satisfied with a COTS product, the image must be formatted according to the requirements of INCITS 385-2004³⁷ and embedded within the CBEFF³⁸ data structure. When an expired card needs to be replaced, a new facial image of the cardholder must be acquired.

Images of the cardholder's right and left index fingers must be stored electronically on the PIV card. The images can be extracted from the full set of fingerprints collected during identity proofing, or new fingerprint images can be acquired. The fingerprints shall be accessible only over the PIV card's contact interface and after the presentation of a valid PIN. Therefore, the images stored on the card must not be readable in the clear and must be protected by another authentication mechanism such as a PIN. Furthermore, FIPS 201 requires the use of an electromagnetically opaque badge holder as another security control that will protect biometric information stored on the card from unauthorized access. The fingerprint images can be used to authenticate a PIV cardholder at the agency's discretion. The facial image is not stored on the PIV card electronically.

The complete technical specifications for the acquisition, formatting, and storage of biometric data are included in NIST SP 800-76.³⁹ Section 4.8 of this handbook includes a detailed biometric device product table.

4.4.3 Biometric Technology Implementation Guidance

FIPS 201 authorizes the use of fingerprint biometric technology to enable Federal agencies to authenticate a PIV card with a high degree of confidence. Furthermore, confidence in a card authenticated by biometric data is higher when the data is used in partnership with another authentication factor, such as a digital signature or a PIN.

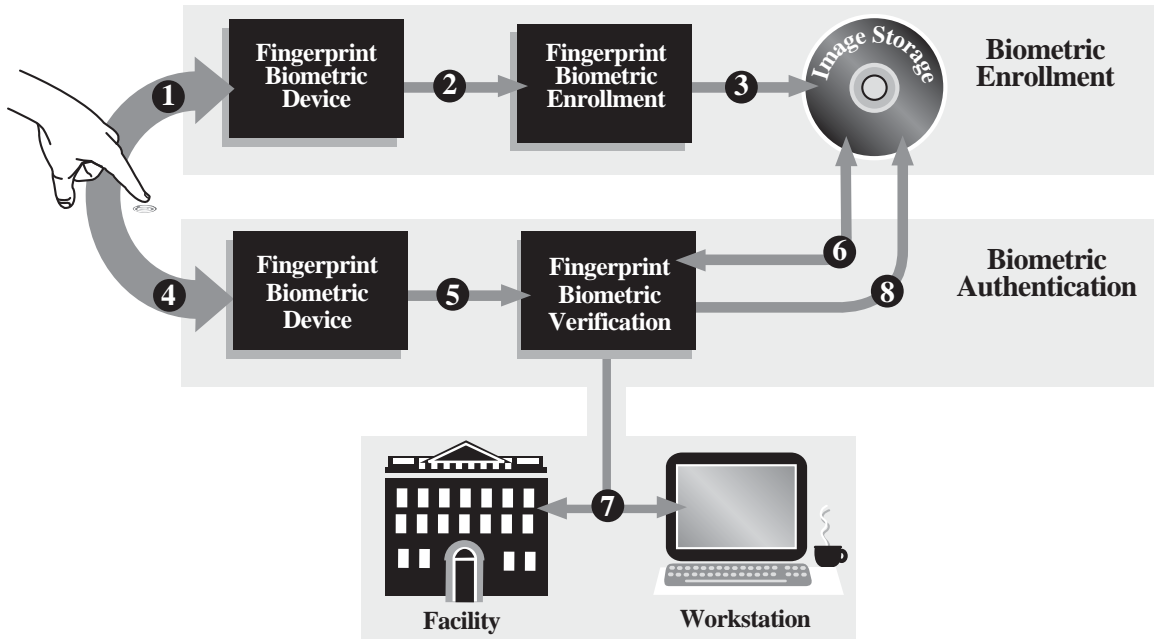
In addition to basic data protection requirements, an agency must consider other requirements before deploying biometrics. Some of the more obvious include how to render accurate and efficient authentication decisions, maintain historic levels of user convenience, and protect users' privacy rights. The use of biometrics has a direct impact on each of these criteria.

Figure 12 illustrates a typical enrollment and authentication process for using fingerprint biometrics as an authentication mechanism. This scenario is applicable to both physical and logical access control applications.

³⁷ INCITS 385-2004, *American National Standard for Information Technology—Face Recognition Format for Data Interchange*.

³⁸ NISTIR 6529-A—*Common Biometric Exchange Formats Frameworks*, NIST Interagency Report, April, 2004.

³⁹ NIST Special Publication 800-76, *Biometric Data Specification for Personal Identity Verification*, NIST, January 24, 2005.



Process	Description
1	Acquire the fingerprint.
2	Format the fingerprint image for storage.
3	Store the image in a data repository (server, reader, or PIV card).
4	Authenticate the fingerprint image stored on the PIV card biometrically by acquiring the verification image.
5	Extract the fingerprint image from the card.
6	Compare the enrollment and verification images.
7	Determine whether the images match. If they match, enable cardholder access. If they don't, send a signal denying access.
8	Create and store a transaction record.

FIGURE 12. FINGERPRINT ENROLLMENT AND AUTHENTICATION PROCESS FLOW

4.4.3.1 Agency Security Considerations

Although the enrollment and capture of fingerprint biometrics is mandatory, agencies must decide for themselves how to actually use biometrics. The list below represents sample criteria that an agency can review to determine whether their operating environments can benefit from the implementation of biometrics:

- Requirement for a high level of security for facilities and systems
- Requirement for a strong mechanism for identity authentication

Federal Identity Management Handbook

- Requirement for a strong identity authentication mechanism where PKI or another mechanism cannot be used
- Business case for the elimination of passwords
- Requirement for enhanced auditing and reporting capabilities
- High percentage of employees who work with confidential or high security information
- High risk of hacker attack on agency systems
- Significant adverse consequences if systems or facilities are compromised

The many different biometric modalities available in the marketplace today satisfy the above requirements to varying degrees; some modalities are more applicable in certain environments than others. With regards to the biometric specifications presented in FIPS 201, fingerprint biometrics are very capable of satisfying each of these requirements and have been integrated into many legacy environments that feature the same requirements. Using fingerprints offers the following advantages:

- **Highly Accurate.** The fingerprint device is a proven technology capable of high levels of accuracy with a long history of use. Used in conjunction with smart cards, fingerprints provide strong protection for the PKI credentials held on the card, thus affording greater trust in PKI services, especially digital signatures for non-repudiation.
- **Versatile Deployments.** Fingerprint capture and authentication devices are small and can easily be integrated into a desktop environment or in a standalone reader. Fingerprint devices can be deployed in a wide range of physical and logical access environments that are susceptible to changes in lighting or climate.
- **Ability to Enroll Alternate Fingers.** FIPS 201 requires that prints of the PIV cardholder's two index fingers be stored on the card. If these fingerprints cannot be obtained, up to eight other fingers are candidates for enrollment.
- **Ease of Use.** The use of electronic fingerprint capture devices requires very little user training. Additionally, such devices are less cumbersome to use than an inkpad.
- **Elimination of Passwords.** Fingerprints can replace passwords for logging on to computer networks, so that users do not have to present a card or remember a password or PIN. This functionality can be beneficial to an agency, since substantial resources are typically required to pay for resetting passwords. Using fingerprints can redirect these resources to other activities.

4.4.3.2 Agency Implementation Considerations

An agency must consider several fundamental implementation decisions before deploying a biometric system. It is highly recommended that an agency first gather the requirements for a biometric system and ensure that they are closely aligned with the agency's objectives for identity management. For example, before the actual details of an implementation are reviewed, define what data the system is designed to protect, how the data will be used by the system, and what fallback procedures can be used during a security breach. The results of this research will yield an optimal balance between security, cost, and the performance of a biometric system. Moreover, the same results can be used to design a

Federal Identity Management Handbook

pilot whose results can be used to gauge how the biometric system will perform in a real-world environment.

The following implementation considerations are specific to a biometric system:

- **False Match/False Non-Match.** The false match rate (FMR) is the rate at which the system incorrectly recognizes an individual as a valid user. The false non-match rate (FNMR) is the rate at which a valid user is rejected by the system. The FMR and FNMR are inversely related, meaning when the FMR goes down, the FNMR goes up, and vice versa. System administrators must balance the FMR against the FNMR to ensure adequate security and user convenience.
- **Enrolled Image Quality.** The quality of the biometric enrollment image is critical to the system's success. If a poor image is captured at enrollment, the likelihood of a false non-match increases substantially. To mitigate the risk of a low quality enrollment image, FIPS 201 recommends that the PIV Issuer match the PIV card applicant's operational biometric with the enrollment biometric when issuing the card.
- **Accuracy Limitations.** Fingerprint biometric systems are highly accurate authentication technologies, but they are subject to failure and can enable an intruder to breach the system. Agencies should consider coupling biometrics with another authentication mechanism, especially in facilities or networks that require a high level of security.
- **Affordability.** The fingerprint biometric market is represented by the greatest number of manufacturers. Market competition and the progressive adoption of fingerprint biometrics have reduced prices significantly. Today, fingerprint biometrics are integrated onto computer keyboards and mice and offered to customers at prices that are only marginally higher than if these peripherals were to be purchased separately.
- **Applicable Standards.** Many biometric solutions use their own proprietary algorithms and processes. The agency must ensure that the biometric solution follows applicable standards to the greatest extent possible.
- **Deployment.** Biometric services can be integrated by an internal agency team, through outsourcing, or through a combination. Agencies can opt to purchase their own biometric system and operate it in-house. In this case, the hardware and software are purchased from a vendor, but the agency staff provides all services. Providing biometric services in-house requires substantial resources, including staff trained in the use of biometric equipment, a trusted computing environment to process and store biometric data, and substantial hardware and software to perform enrollment and template creation, capture, translation, and verification.
- **Enrollment.** During enrollment, the PIV applicant's required information is captured, including biographic data, photograph, and biometric fingerprint image. Best practices encourage a linear process, in which the applicant's information is gathered and vetted, and a PIV card is issued once the background check and adjudication process is completed. Card enrollment can be performed locally or centrally. In local enrollment, card personalization and distribution are performed on site. In central enrollment, the biometric image must be downloaded to the card issuance facility. Local enrollment is often faster than centralized enrollment but requires the purchase of more equipment.

- **Comparison Processing.** Processing that uses biometrics requires that the data presented be compared to captured data. This comparison can be performed on a PIV card itself, on the card reader, or on a central server. Each solution offers different security levels and processing speeds.

4.4.3.3 Agency Policy Considerations

In addition to security requirements, agencies should consider functional and policy issues when deciding whether to use fingerprint biometrics. The agency's biometric requirements should also be communicated to users so that users know how they can use biometrics to improve work performance and how agencies will be protecting biometric data. The ultimate success of a biometric system depends on how well an agency's administrators and user population understand why and how biometrics are used. The following criteria represent some relevant biometric policy considerations:

- **User Acceptance.** Fingerprint technology's association with forensic and criminal fingerprinting may make some users uncomfortable. Agencies should stress the underlying value of biometrics, such as security and ease-of-use.
- **Privacy.** Privacy advocates are concerned that fingerprint data may be used for activities outside of an agency's access control system. Agencies should educate users and organizations on their processes for securing biometric data and ensure that the data is not vulnerable to "function creep."
- **Inability to Enroll Some Users.** A small percentage of users will be unable to enroll in many fingerprint systems. Agencies should identify a fallback authentication method to authenticate such users. For example, PKI or a password may be a suitable substitute.
- **Ease of Use.** Users have established expectations for the convenience and speed of using access control systems. Fingerprint devices should strive to maintain equivalent ease of use.

4.5 Card Reader Specifications

4.5.1 Smart Card Readers

Card readers are the electronic devices that supply power to and communicate with the PIV card. Card readers enable the cardholder to be authenticated and also communicate with the back-end registration system for an access control application. The card-to-reader interface represents an important consideration in a credentialing system's architecture. It establishes parameters for electronic signals and transmission protocols that determine how a PIV card communicates with the reader and other components of the access control system.

To be compliant with FIPS 201, card readers must be compatible with the specifications of the International Organization for Standardization (ISO). This decision is fortunate: ISO standards governing the card-to-reader interface have been public for several years, so card-reader vendors have had ample time to manufacture compliant products. As a result, many available COTS readers are already compliant. These readers are interoperable with each other, as required by the ISO specifications.

4.5.2 Card Reader Compliance Requirements

FIPS 201 defines specifications for both contact and contactless interfaces. At a minimum, agencies must adhere to these specifications when selecting card readers.

4.5.2.1 Contact Reader Specifications

According to FIPS 201, contact card readers must comply with ISO/IEC 7816, the standard for the card-to-reader interface.⁴⁰ ISO/IEC 7816 is composed of a series of standards defining the parameters for use of ICCs with a contact interface. When the reader is connected to a desktop computer, the reader must also comply with the Personal Computer/Smart Card (PC/SC) specification for the reader-to-host system interface.

4.5.2.2 Contactless Reader Specifications

According to FIPS 201, contactless card readers must comply with ISO/IEC 14443, the standard for the card-to-reader interface.⁴¹ ISO/IEC 14443 is composed of a series of standards defining the parameters for use of integrated circuit cards with a contactless interface. When the contactless reader is connected to a desktop computer, the reader must also comply with the PC/SC Specification for the reader-to-host system interface.

4.5.3 Card Reader Implementation Guidance

As agencies prepare to deploy their card readers, they will be able to leverage the ISO specifications, which establish uniformity and interoperability. However, although all ISO-compliant card readers are interoperable, an agency should be sure that the readers it procures are also compatible with the agency's PIV card. Therefore, agencies should not simply procure the card readers and integrate them at their facilities prior to ensuring their compatibility with PIV cards. Until smart card manufacturers are able to issue PIV-compliant cards, sufficient uncertainty will remain as to whether the PIV cards will be compatible with card readers. This issue warrants concern and caution on behalf of agencies.

FIPS 201 describes several candidate card authentication mechanisms that can be used to satisfy different security requirements. The card reader an agency selects must offer the functionality required to support the chosen authentication mechanism. For example, if an agency decides to use a biometric and PIN to authenticate users to a highly secure room, it will have to acquire a combination card reader that includes both a biometric acquisition scanner and a PIN pad. This card reader model will require a contact interface as FIPS 201 specifies the use of biometrics over the contact interface only.

The Federal Government is aware that commercially available cards cannot currently meet the FIPS 201 requirements. Smart card manufacturers are working to remedy this situation. To ensure that smart cards and readers are compatible, the government is sponsoring conformance testing at the Department of Defense Joint Interoperability Test Command (JITC). The initial testing results are to be published in August 2005. (For more information on the conformance test suite and smart card technologies being tested, refer to Section 5.6.)

⁴⁰ FIPS PUB 201, op. cit.

⁴¹ Ibid.

4.5.3.1 Agency Implementation Options

As the state of today's Federal identity management systems runs the entire credentialing gamut—from agencies in the midst of requirements gathering to those that are in full-scale production—agencies are able to choose from several courses of action to prepare their operational environments for FIPS 201-compliant card readers. These options are as follows:

- **Begin the Planning and Analysis Phase.** According to the OMB Implementation Guidance, agencies are required to be in compliance with the FIPS 201 technical specifications by October 27, 2006. This interval of time may be used by agencies to focus on planning and designing a PIV system. Since the results of the conformance testing of vendor products, including smart-card readers, should be available starting in August 2005, agencies that are not currently using smart-card readers can use this time to analyze and formulate their card-reader requirements. Careful planning will lower the risk of deploying incompatible readers. This scenario most likely pertains to agencies that are currently not using smart-card readers.
- **Maintain Current Operations.** Agencies that have already deployed smart-card readers should continue to use their installed readers. They should simultaneously identify which of their installed readers comply with FIPS 201 and which do not. Nonconforming readers can be identified by contacting the card reader vendor, or the agency can wait for the JITC conformance testing results. Agencies that are currently deploying smart cards should consider continuing their deployment. These cards are already interoperable with the installed base of smart-card readers. As such agencies begin deploying PIV-compliant smart cards, they may need to upgrade or reprogram their readers. Such agencies should consult with the manufacturer to determine whether their installed smart-card readers are programmable. If they are not, the readers will most likely require replacement. Finally, such agencies should create a migration plan for adopting ISO-compliant readers.
- **Evaluate FIPS 201-Compliant Readers.** FIPS 201-compliant readers are currently commercially available, so an agency may consider deploying them immediately. However, there are still significant risks surrounding card-to-reader interoperability. Product guarantees will not be available until the JITC conformance testing is completed. An agency that chooses this option should include protective clauses in its contracts with the smart card and card-reader vendors so that the agency has legal recourse if interoperability fails.

4.5.3.2 Balancing Security with Convenience

Imbedded within many identity management technologies is an inherent trade-off between security and convenience: as security levels increase, user convenience decreases, since longer card-authentication processing periods are required for users to access facilities and networks. Conversely, systems that support high levels of user convenience by authenticating cards rapidly may sacrifice a measure of security. Smart-card readers are no exception. Federal agencies should regularly evaluate their operational environment so that a balance is struck between security and user convenience.

Figure 13 illustrates how an agency may define its card reader assurance levels by comparing the facilities and information that concentric security circles are designed to protect with throughput levels. Concentric security circles are the rings of security that help determine the assurance level required for

the protection of a specific environment’s assets. For technical implementation guidance on designing card reader assurance levels, refer to the PACS Implementation Guidance.⁴²

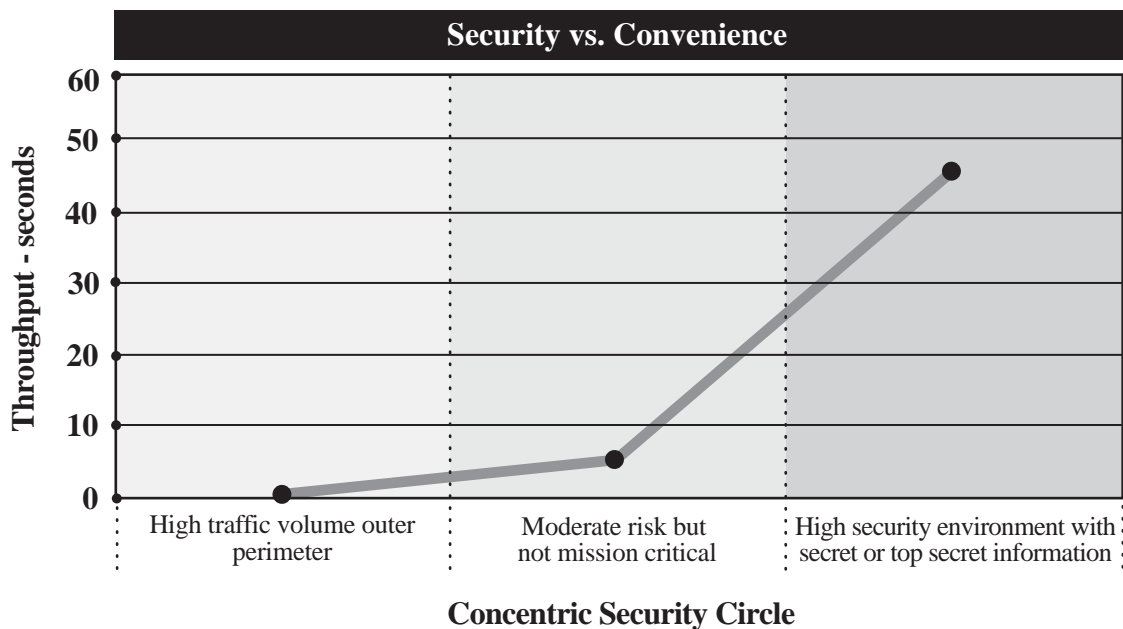


FIGURE 13. BALANCING CARD READER ASSURANCE LEVELS WITH CONVENIENCE

4.6 PIV II – Identity Proofing, Registration, Issuance and Management

To achieve compliance with PIV II requirements, an agency must be issuing PIV cards that comply with the Government’s PIV II interoperability specifications. This requirement does not apply to existing government identity credentials, but only to newly issued PIV cards. All requirements for PIV I compliance must be met for PIV II.

Additional security requirements are also imposed for PIV II. Detailed technical specifications for PIV II compliance are provided in SP 800-76 and SP 800-73. Following is a summary of the PIV II requirements for identity proofing, issuance, maintenance, and key management for an interoperable PIV card.

4.6.1 PIV II Identity Proofing and Registration Requirements

PIV II credential issuance can be performed only after all requisite PIV I identity-proofing and background check steps have been successfully performed and documented. An additional requirement for PIV II compliance is that the fingerprints and facial biometrics that are used to personalize the PIV card must be captured during the identity proofing and registration process and re-verified during the issuance process. Therefore, agencies will need to procure biometric capture devices and deploy them to those responsible for identity proofing and registration within the agency. Biometric specifications are included in SP 800-76. When agencies capture the biometric data from the applicant it is recommended that they implement some type of secure identity management system that

⁴² Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems V2.2, Government Smart Card Interagency Advisory Board, July 30, 2004.

stores the biometric information and is capable of securely providing the biometrics to the card production and personalization system.

Figure 14 illustrates how an agency may chose to design identity proofing and issuance systems, including the identity management system, and integrate the various roles associated with identity proofing and card issuance.

PIV Identity Verification and Issuance

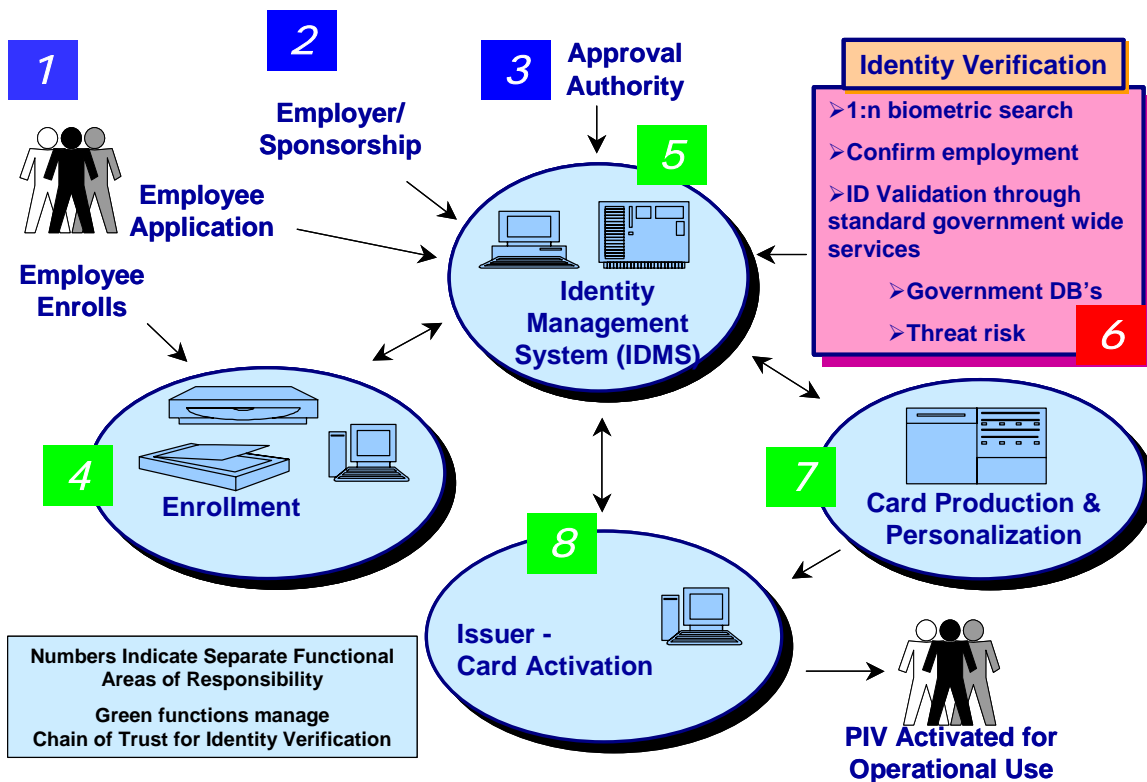


FIGURE 14. PIV IDENTITY VERIFICATION AND ISSUANCE

The identity-proofing and registration requirements are as follows:

1. Identity proofing and registration systems must comply with the objectives and requirements in Section 2.2 of FIPS 201 (Section 2.1 of this document).
2. Applicant biometric information used for card personalization must be captured during the identity proofing and registration process.

4.6.2 PIV II Card Issuance Requirements

The card issuance requirements for PIV II compliance are listed below. All of the PIV I issuance requirements must be followed except as noted.

Federal Identity Management Handbook

1. Issuance and maintenance systems must comply with the objectives and requirements in Section 2.3 of FIPS 201 (Section 2.3 of this document).
2. The PIV card must be revoked if the NACI is not successfully completed and adjudicated within 6 months of the application or the results are deemed to be non-satisfactory by the issuing agency.
3. Individuals within an agency responsible for issuance must perform a one-to-one fingerprint biometric match of the Applicant against the enrollment record or the PIV card before releasing the PIV card to the Applicant.

The one-to-one fingerprint biometric check provides added assurance in the binding of the applicant's identity to the PIV card. Individuals within agencies responsible for PIV card issuance will need to have biometric fingerprint devices and connectivity to the identity management system to perform the one-to-one fingerprint biometric match. If agencies choose to match the Applicant's fingerprint biometric to the card, PIV Issuers will need PIV card readers to perform the check.

Agencies are free to implement more stringent requirements or agency specific requirements as long as the requirements above are satisfied.

Card Issuance Implementation Recommendations

4.6.2.1 Card Issuance Components

The components necessary for PIV card issuance may include the following:

- PIN pad
- Camera
- Card printer
- Fingerprint biometric capture device
- Network connectivity
- Desktop computer and keyboard

These items should be included in the acquisition plan that each agency will compile for FIPS 201.

Certain issuing components that can be shared by multiple issuing stations. For example, depending on the logistics involved, issuing stations may be able to share a card printer or the camera used to take the applicant's photograph. Sharing components can decrease overall implementation costs, although, there may be a trade-off in the form of increased wait times for PIV card issuance and thus decreased customer satisfaction. How to configure issuing stations should be decided by determining how many applicants will be issued a PIV card at the particular site.

4.6.2.2 PIV Card Activation⁴³

Before a PIV II compliant PIV card can be issued, it must be personalized with the PIV applicant's information and activated. To activate the card, the card management system performs a challenge-response protocol using cryptographic keys stored on the card. When cards are personalized, card management keys are set to be specific to each PIV card (a card issuer may not use a single cryptographic key to activate more than one card). This requirement eliminates the possibility that if one key used for activation is compromised, all PIV cards are compromised as well. Card management keys must meet the algorithm and key size requirements stated in Section 0.

4.6.2.3 PIV Card Personalization

The PIV card is personalized with the applicant's information during card activation. Personalization occurs when the card body is printed with the mandatory PIV credential topology elements and the ICC is populated with the mandatory logical data elements. (The acquisition of card personalization equipment is discussed in Section 4.8.) Card personalization can occur prior to the Applicant's appearance before the PIV Issuer or in conjunction with the Applicant's appearance at the issuing station.

The PIV card is personalized using the information provided by the Applicant and Approver during the application process and captured during the registration process. There are several ways for the PIV registration process to collect and distribute this information to the PIV issuing process:

- Through a secure web-based⁴³ application associated with the agency's identity management system
- Through an encrypted e-mail message
- Through secure personal delivery (e.g., the PIV Registrar hand delivers the applicant's information to the PIV Issuer)

If an IDMS is implemented, the IDMS transmits personalization information to the card production and personalization system via a secure channel.

The Applicant's personal information must be communicated securely. Agencies should ensure that all individuals involved in the issuance process have been thoroughly vetted, the data transfer is secure, and all applicable privacy standards are maintained.

4.6.3 PIV Card Maintenance

Certain card maintenance functions may be necessary during the life of the PIV card. These functions are essential to the management of a PIV card. Maintenance functions can include:

- PIV card renewal (PIV card reaches the end of life)
- PIV card reissuance (PIV card is lost, stolen, or compromised)
- PIV card PIN reset (the PIN on a PIV card is locked because the predefined number of attempts to enter the PIN is exceeded)

⁴³ FIPS PUB 201, op. cit.

Federal Identity Management Handbook

- PIV revocation or termination (an individual is fired from or voluntarily leaves an organization)

Each of these card management processes is detailed below.

The sole card maintenance requirement is that individuals within an agency responsible for authenticating PIV cardholders must have access to the status of PIV credentials in real time. For example, if an individual's employment is terminated, *all* individuals and systems within that agency responsible for authentication of PIV credentials need to be informed *immediately*, such that the individual who was terminated cannot access any of the agency's logical or physical assets.

4.6.3.1 Card Renewal

Card renewal replaces a card repeating the full identity proofing and registration process (for example, when an individual's PIV card expires). The card renewal requirements are as follows:

1. The PIV Issuer will validate that the individual has all necessary identity documents on file and that the individual's card has not been revoked, suspended, or terminated.
2. NACI checks must be followed in accordance with OPM guidance.
3. PIV cards are only valid for a period of 5 years.
Individual agencies are free to implement a shorter life cycle for their PIV cards.
4. A PIV cardholder should be permitted to apply for a PIV renewal 6 weeks prior to expiration of the PIV card or at an earlier time as determined by individual agencies.
5. The PIV Issuer will verify the cardholder's identity against the biometric information stored on the expiring card.
6. The expired PIV card must be collected by the PIV Issuer and destroyed.
7. Fingerprints change very little over the course of a person's life; therefore, the same fingerprint data can be reused with the new PIV card.
8. The digital signature must be recomputed with the new FASC-N. Every PIV card must have a unique FASC-N.

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

Agencies will want to establish a method by which all collected PIV cards are destroyed. It is not a good business practice to collect expired cards and store them for long periods of time without destroying them; these cards could be misplaced or stolen. Following is an example business process that agencies could implement:

1. An agency designates an organizational component to be responsible for PIV card destruction.
2. The agency schedules delivery of the PIV cards to that component (e.g., every Friday or once every two weeks).

Federal Identity Management Handbook

3. PIV cards are either hand-delivered or mailed to the component using a secure delivery method.
4. The component then destroys the cards according to agency policies. Agencies should ensure that the data in the ICC is electronically erased and all other data elements used to identify an individual are destroyed.

4.6.3.2 PIV Card Reissuance

When a PIV card is reissued, the entire registration and issuance process, including fingerprint capture, is conducted. The PIV Issuer shall verify that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.

The following requirement applies to card reissuance:

1. A cardholder shall apply for reissuance under the following circumstances:
 - The PIV card is reaching its expiration date. Up to 6 weeks prior to expiration a card can be renewed.
 - The PIV card is expired.
 - The PIV card is compromised, lost, or stolen.
 - The PIV cardholder's employee status changes (e.g., promotion) or an attribute changes.
 - The PIV cardholder's logical credentials are compromised.

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

- The PIV card is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status.
- The CA must revoke the certificate corresponding to the PIV authentication key on the PIV card. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. Certificate revocation lists (CRLs) shall include the appropriate certificate serial numbers.
- Online Certificate Status Protocol (OCSP) responders shall be updated so that queries with respect to certificates on the PIV card are answered appropriately. This may be performed indirectly (by publishing the CRL) or directly (by updating the OCSP server's internal revocation records).
- For attribute changes, the PIV Registrar must verify the reason for the change and keep a copy for records.

If the old PIV card is still available, it should be collected and destroyed in accordance with agency specific policies. If the card cannot be collected, normal operational procedures for revoking the old credential shall be completed within 18 hours of notification. Under some circumstances, 18 hours is an unacceptable delay; for example, a department or agency may discover a cardholder is a person on a terrorist watch list. In that case, emergency procedures must be executed to disseminate this information to law enforcement personnel as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications for such cases.

4.6.3.3 PIV Card PIN Reset

The PIN on a PIV card may need to be reset if the contents of the card are locked because an invalid PIN was entered more than the number of attempts stipulated by the department or agency. Generally, it is a best business practice to allow a cardholder three attempts to enter the PIN correctly. The PIV issuer can perform PIN resets or another individual may be designated to perform that function with in the individual agency.

The PIN reset requirement is as follows:

1. Before the reset PIV card is given back to the cardholder, the individual responsible for PIN reset (i.e. PIV issuer) should ensure that the cardholder's biometric matches the stored biometric on the reset PIV card.

Departments and agencies can adopt more stringent procedures for PIN reset (including disallowing PIN reset, and requiring the termination of PIV cards that have been locked). Individual agencies should formally document their procedures for PIN reset.

Many agencies that are currently deploying smart card-technology have found that requests for PIN reset is a major help desk expense. Agencies must provide individuals to respond to cardholder requests to have PINs reset.

4.6.3.4 PIV Card Termination

The termination process ensures that a PIV card can no longer be used. The termination requirement is as follows:

1. The PIV Card shall be terminated under the following circumstances:
 - An employee separates (voluntarily or involuntarily) from Federal service.
 - An employee separates (voluntarily or involuntarily) from a Federal contractor.
 - A contractor changes positions and no longer needs access to Federal buildings or systems.
 - A cardholder is determined to hold a fraudulent identity.
 - A cardholder passes away.

Termination procedures must be in place as to ensure the following:

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

Federal Identity Management Handbook

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

PIV card termination is the last process in the lifecycle of a PIV card.

4.6.4 Key Management

Key management comprises the policies and procedures for managing data required to establish and maintain cryptographic keys. For the cryptographic system to be successful, the keys must be protected at all times. By implementing a competent key management process, an agency can establish a foundation for secure generation, storage, distribution, and revocation of keys. An agency's key management process should be documented in the agency's Certification Practice Statement (CPS), which describes the practices for implementing the agency's PKI. The CPS may be created by a shared service provider (see Section 5.1.6) or by the agency itself.

FIPS 201 requires agencies to issue and manage X.509 public key certificates for the management of public keys stored on the PIV card. Certificates must be issued according to the guidelines provided in the *X.509 Certificate Policy for the Common Policy Framework* (PKI Common Policy).⁴⁴ The PKI Common Policy is a Federal policy that agencies can reference when designing and implementing their PKI systems. The OMB approved this policy and advocates its use.

The PKI Common Policy describes a concise methodology for implementing the following PKI services:

- Key generation/storage
- Certificate generation, update, renewal, re-key, and distribution
- CRL generation and distribution
- Directory management of certificate-related items
- Certificate token initialization/programming/management
- System management functions (security audit, configuration management, archiving)

These services must accompany the implementation of key cryptography. An agency must enable these services regardless of whether it implements only the mandatory key or both the mandatory key and the optional keys.

4.6.4.1 FIPS 201 Key Management Requirements

FIPS 201 requires agencies to use the PKI Common Policy as guidance for digital certificate management. The following sections summarize the major components of the guidance.

⁴⁴ *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*, February 10, 2004.

4.6.4.2 PKI Common Policy Requirements

4.6.4.2.1 Application for a Certificate

When a prospective subscriber applies for a certificate, an agency must complete several steps before issuing the certificate. This process varies slightly, depending on whether the subscriber is a Federal employee, a contractor, or another affiliated user. For a detailed description of the PKI identity-proofing process, refer to Section 5.1 of FIPS 201 and Section 2.2.1 of this handbook.

4.6.4.2.2 Certificate Issuance

FIPS 201 requires the agency's CA to participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-signed, self-issued, and CA certificates issued by CAs shall conform to the following worksheets found in the *X.509 Certificate and CRL Profile for the Common Policy*⁴⁵:

- Worksheet 1: Self-Signed Certificate Profile
- Worksheet 2: Self-Issued CA Certificate Profile
- Worksheet 3: Cross Certificate Profile

The PKI Common Policy requires FIPS 140-2⁴⁶ Level 2 validation for the PIV card. FIPS 201 has imposed an additional security measure by requiring PIV cardholders to authenticate to the PIV card each time the card performs a private key computation with the digital signature key.

The certificate issuance process begins when the subscriber's identification data is bound to the public key. An agency can bind the data electronically, with cryptography, or with a hardware cryptographic module. This decision should be based on the agency's business rules for certificate issuance.

FIPS 201 and the PKI Common Policy support the use of both RSA and elliptic curve cryptographic algorithms. Where an asymmetric card authentication key is accessible through the contactless interface, the elliptic curve algorithm offers compelling performance advantages. Private key operations may be performed with fewer operations than with RSA, and the encrypted challenge and the public key certificate will be smaller. To maximize performance, agencies should consider the 163-bit elliptic curve algorithms for the asymmetric card authentication key. However, agencies should note that elliptic curve authentication mechanisms are not widely implemented at this time. Agencies should not depend upon PIV cards issued by other agencies supporting elliptic curve card authentication keys.

For the PIV authentication key, digital signature key, and the key management key, the RSA algorithm offers compelling advantages with respect to interoperability. To the first order of approximation, all applications that support asymmetric cryptography support the RSA algorithm. Implementations may limit the size of their private keys, but support for larger public key sizes is also prevalent. These keys are accessed solely through the contact interface and require cardholder activation (e.g. by entering a PIN). Consequently, the differences in performance do not have the same effect on usability for these keys. To maximize their utility, agencies should use the RSA algorithm for the PIV authentication

⁴⁵ *X.509 Certificate and CRL Profile for the Common Policy*, Version 1.1, July 8, 2004.

⁴⁶ *Federal Information Processing Standards Publication 140-2*, May 25, 2001.

Federal Identity Management Handbook

key, digital signature key, and the key management key until 2008, to give application developers time to add elliptic curve support.

When the CA receives a request to issue a certificate, it verifies the identity and authority of the subscriber submitting the request and reviews the assurance level used to protect the request. The CA then builds and signs the digital certificate and notifies the subscriber that it is available. Once the subscriber is ready to accept delivery of the certificate, the CA generates the private key in a cryptographic module and instantiates the data onto a cryptographic token. The token is sent to the subscriber, and the subscriber acknowledges receipt of the token.

The last step in the certificate issuance process is to distribute the CA's public key. While public keys are commonly known as the originators of certification paths, the CA must first ensure the integrity of its trust anchor or trusted certificate, because this is where the public keys reside. Therefore, the CA must validate that subscribers have received certificates through a trusted certificate.

The PKI Common Policy suggests the following ways to deliver trusted certificates to subscribers:

- The RA loads the trusted certificate onto a token through secure mechanisms.
- The certificates are distributed using secure out-of-band mechanisms.
- Certificate hashes or fingerprints are compared to trusted certificate hashes or fingerprints.
- Certificates can be loaded from web sites secured with a valid certificate of equal or greater assurance level than the trusted certificate.

4.6.4.2.3 Certificate Acceptance

An agency is responsible for communicating a code of conduct to subscribers that will ensure their correct use of digital certificates. Specific guidance should be provided for safeguarding private keys at all times, notifying the CA in the event that private keys are compromised, and abiding by the terms and conditions pertaining to certificate use. These responsibilities should be documented in the agency's Certificate Policy. After these terms are satisfied, the agency informs the subscriber that a certificate has been generated successfully.

4.6.4.2.4 Certificate Suspension and Revocation

Certificate suspension or revocation occurs when the subscriber's binding to the public key in the certificate (established during the identity-proving process) is severed. For example, a subscriber's role classification can be altered, which may affect certificate-signing privileges; a private key may be compromised; the subscriber may violate the user agreement; or a subscriber may change positions or employment altogether.

To mitigate the potential risk of fraudulent activity, it is imperative that CAs revoke certificates as soon as revocation requests are approved. Therefore, no grace period is allowed for certificate revocation. Moreover, the PKI Common Policy encourages agencies to update their CRLs every 18 hours. The PKI Common Policy also mandates the CRL publication frequencies shown in Table 8.

Table 8. Mandated CRL Publication Frequencies

Use Case	CRL Publication
CAs operating off line	Every 24 hours
Subscribers operating on line	Every 18 hours
Certification revocation due to compromise	Within 6 hours of notification

4.6.4.2.5 Security Audit Procedure

The CA is responsible for generating and monitoring audit log files. Agency CAs are required to capture the following information in each audit record to ensure compliance with the PKI Common Policy:

- The type of event
- When the event occurred (date and time)
- An indication of whether the CA’s signing process succeeded or failed
- An indication of whether certificate revocation succeeded or failed
- The identity of the entity and/or operator that caused the event

Examples of auditable events include identification and authentication attempts, key generation, certificate registration, certificate revocation, and CRL profile management. (A comprehensive list of events is available in the PKI Common Policy.)

PKI authorities are encouraged to review audit logs at least once every 2 months, with careful consideration of any unusual records.

4.6.4.2.6 Records Archival

Each agency’s PKI administrator is required to maintain an archival database that provides storage capabilities for all transaction records enabled by PKI. The archive must reside in a location that is physically separate from the CA. Records stored in the archives must be maintained for a minimum of 10 years and 6 months. Proper management of this database is critical to the success of PKI, because the availability of a long-term audit trail can allay many liability risks.

The PKI Common Policy has established the following minimum requirements for the content of an agency’s PKI archives:

- CA accreditation (if applicable)
- Certificate Policy
- Certification Practice Statement
- Contractual obligations
- Other agreements concerning operations of the CA
- System and equipment configuration

Federal Identity Management Handbook

- Modifications and updates to system or configuration
- Certificate requests
- All certificates issued and/or published
- Record of re-keys
- Security audit data
- Revocation requests
- Subscriber identity authentication data
- Subscriber agreements
- Documentation of receipt of tokens
- All CARLs and CRLs issued and/or published
- Other data or applications to verify archive contents
- Documentation required by compliance auditors

4.6.4.2.7 Compromise and Disaster Recovery

The CA and its associated directory are designed to operate 24 hours a day, 365 days a year. While this is an optimal goal, it must be anticipated that technological, human, or other problems will affect the CA's operations.

To help agencies prepare a plan that addresses potential problems with the CA, the PKI Common Policy includes several scenarios in which CA performance is significantly affected and suggests possible responses. These scenarios are listed in Table 9.

Table 9. Scenarios Affecting CA Performance and Recommended Responses

Scenario	Response
CA equipment is damaged	Notify the Federal PKI Policy Authority. Attempt to restore CA operations within 72 hours.
CA cannot generate CRLs	Notify the Federal PKI Policy Authority. Attempt to restore CA operations within 72 hours.
CA signature keys are compromised	Notify the Federal PKI Policy Authority and other cross-certified CAs. Attempt to restore CA operations within 72 hours. Distribute the new trusted certificate through a secure out-of-band mechanism. Automatically renew subscriber certificates or require subscribers to apply again.
CA is extensively damaged and all copies of the CA signature key are destroyed	Notify the Federal PKI Policy Authority. CAs can continue to use original certificates while the new certificates are being generated.

4.7 Card Authentication

Authentication is the process that determines whether an individual or entity is actually what it appears to be. Authentication seeks to establish the validity of an identity claim. For the purposes of this document and FIPS 201, the term “authentication” is used in reference to the identity of the cardholder.

For credentials issued by different agencies to be accepted throughout the Federal Government, an agency must have confidence in a credential issued by a different agency. For agencies to have confidence in each other’s credentials, the Federal Government has defined a set of *identity assurance levels* that apply to the methods used for authentication. Each identity assurance level guarantees the particular amount of confidence an agency can have in the identity of any PIV cardholder, even if the card was issued by a different agency. Each level of identity assurance is achieved by using particular methods to authenticate the cardholder and the card.

Each agency is responsible for assigning a PIV assurance level to both their physical and logical resources. After agencies have assigned an assurance level they can then use the appropriate authentication mechanism to provide the required level of identity assurance.

4.7.1 Identity Authentication Assurance Levels

FIPS 201 defines three PIV identity assurance levels. The three levels are similar to the four assurance levels defined in OMB’s E-Authentication Guidance, M-04-04, for Federal agencies. Table 10 compares the OMB and PIV assurance levels.

Federal Identity Management Handbook

Table 10. OMB E-Authentication and PIV Assurance Levels

OMB E Assurance Levels		PIV Assurance Levels	
Level		Level	
1	Little or no confidence in the asserted identity's validity.		No equivalent.
2	Some confidence in the asserted identity's validity.	Some	A basic degree of confidence in the identity of the cardholder.
3	High confidence in the asserted identity validity.	High	A strong degree of confidence in the identity of the cardholder.
4	Very high confidence in the asserted identity's validity.	Very High	A very strong degree of confidence in the identity of the cardholder.

The PIV authentication levels do not include a level that is equivalent to OMB E-Authentication Guidance, M-04-04 Level 1 assurance. One of the goals of FIPS 201 is to ensure that a basic level of identity assurance is associated with every PIV cardholder. Therefore, it would be counterproductive to permit a level of assurance that did not at least include some confidence in the identity of a PIV cardholder.

Three parameters establish confidence in the identity of the PIV cardholder:

- The thoroughness of the identity-proofing process implemented by agencies.
- The security of the PIV card issuance and maintenance process implemented by agencies.
- The technical authentication mechanisms, which are used to verify that the PIV cardholder is the rightful owner of that PIV card. Each mechanism involves the use of specific processes and techniques.

Individual agencies are responsible for determining the proper level of identity assurance required for access to their physical and logical assets. This determination should be based on a worst-case scenario; for example, to mitigate the risk that individuals could gain access to physical or logical assets as a result of their identity being improperly authenticated. Agencies should evaluate the potential negative repercussions to determine the proper level of identity assurance required.

For example, suppose that an agency has a facility in which only office supplies are stored—things such as computer paper, pens, and ink cartridges for printers. The agency should evaluate what the repercussions might be if an improperly authenticated individual were able to access the facility. In this case, the consequences of improper authentication may be minor, so an agency would want to assign the PIV authentication level *some confidence*. Conversely, a facility that stores personnel records will most likely require a PIV authentication level of *very high confidence*. This is because improperly granting access to the facility and the records could have serious consequences.

OMB M-04-04 addresses identity assurance for electronic transactions and describes a methodology for addressing the risks and potential impact of falsely authenticating an individual's identity.⁴⁷ A full text version of OMB M-04-04 is located at <http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>. FIPS 201 requires that the methodology described in OMB M-04-04 be applied by agencies when

⁴⁷ FIPS PUB 201, op. cit.

authenticating individuals who can access logical resources. When authenticating individuals for physical access, agencies can use a methodology similar to that described in OMB M-04-04 or another methodology entirely, such as the IAB PACS v2.2. To help reduce the risks and potential impact of falsely authenticating an individual for physical access, agencies should at a minimum ensure that security personnel are properly trained. The training should cover the common characteristics of a PIV card, including the data printed on the card and the data stored in the ICC. Training should also be provided to security personnel on the functionality of a PIV card. Lastly, the components used to support physical access should be auditable.

4.7.2 Card Authentication Mechanisms

A PIV card supports multiple authentication mechanisms in both reader and reader-less environments. The environment dictates which authentication mechanisms can be implemented. For example, at a physical access point with a security guard but no PIV card reader, the PIV cardholder can only be authenticated by visual inspection of the PIV card. Generally, the higher the degree of identity assurance, the longer the authentication transaction. For example, it may take less time to visually authenticate an individual than it does for an individual to enter a PIN and present a fingerprint biometric for authentication, although visual authentication is considered a weak form of authentication.

The authentication mechanisms supported by a PIV card include the following:

- Visual authentication
- CHUID authentication
- Biometric authentication
 - Unattended biometric authentication
 - Attended biometric authentication
- PKI authentication

For planning purposes, agencies should be aware that there are certain long-term costs associated with implementing authentication mechanisms and that some authentication mechanisms may be more costly than others over the long term. As an example, in the long term, visual authentication may be more costly to implement than biometric authentication. Visual authentication requires the services of a security officer at each physical access point to visually inspect the identification card and cardholder. Unattended biometric authentication requires biometric readers at physical access points and, depending on where an agency wishes the biometric match to take place (in the reader, on the card, or in a database), network connectivity. The unattended biometric authentication mechanism is a one-time expense with reoccurring maintenance and upgrade costs. The cost of the security official is usually a reoccurring expense. At some point, the cost of implementing visual authentication should surpass that of implementing unattended biometric authentication.

Each authentication method has certain advantages and disadvantages, summarized in:

Table 11. Advantages and Disadvantages of Authentication Methods

Visual Authentication	CHUID Authentication	Biometric Authentication	PKI Authentication
<p>Not conducive to high throughput areas.</p> <p>Can be used in reader and reader free environments.</p> <p>Non-card owner may be detected by visual inspection by security officer.</p>	<p>Conducive for use in high throughput areas.</p> <p>Can only be used in environment with electronic readers (contact or contactless).</p> <p>Non-card owner cannot be detected (CHUID can be read without cardholder activation)</p>	<p>Can be slow because use of biometric requires cardholder to enter PIN number and provide biometric.</p> <p>Can only be used in an environment with contact readers.</p> <p>Non-card owner can be detected.</p>	<p>Can be slow because use of PKI requires interaction with card holder (cardholder required to enter PIN).</p> <p>Typically only used in a contact reader environment.</p> <p>Non-card owner can be detected. PIN is required to access the PKI certificate.</p>

4.7.2.1 Visual Authentication

Visual authentication provides *some confidence* in the identity of a cardholder.

Several elements can be used for visual authentication, including a photograph, name, employee affiliation/employment identifier, expiration date, agency card-serial number, and issuer identification. An agency may also choose to implement and use several optional visual elements, such as a cardholder signature or cardholder physical characteristics. Because it is prone to human error, visual authentication provides the lowest level of identity assurance.

Agencies may not want to install electronic readers at all physical access locations, or it may not be feasible for agencies to have connectivity at all physical access locations. Under these circumstances, agencies can implement visual authentication of a PIV cardholder. The visual authentication process should at a minimum follow these steps:

1. The security officer at the physical access entry point confirms that the PIV card presented by the PIV credential holder appears to be valid and unaltered.
 For a security officer to check the validity of a PIV card and determine whether it is unaltered, the officer will need training on the physical characteristics of the PIV card.
2. The security officer compares the photograph on the PIV card to the face of the individual presenting the card.
3. The security officer checks the expiration date on the PIV card to ensure that the card is still valid.
4. One or more of the other visual data elements should be used to determine whether the PIV cardholder should be granted access.

If agencies choose to implement certain optional visual elements, the officer could also use the following for authentication:

Federal Identity Management Handbook

- Check the physical characteristics on the card to ensure that they describe the individual presenting the card.
- Collect the PIV cardholder's signature and compare it with the signature on the card.

People never sign their signature the same way twice. Therefore, if the visual authentication process includes evaluating the PIV cardholder's signature with the signature on the card, security officials need proper training in detecting false signatures.

4.7.2.2 CHUID Authentication

A PIV cardholder can be authenticated electronically using the CHUID stored in the PIV card ICC. Because the CHUID is a free-read data element, it provides only *some confidence* in the identity of the cardholder.

Implementation of PIV II in FIPS 201 requires that all PIV cards contain a CHUID. If authentication is accomplished using the CHUID, a FIPS 201-compliant PIV card reader must be installed at the access point. Both contact and contactless readers can read the CHUID. The CHUID can be used to authenticate a PIV cardholder using the following process:

1. The CHUID is read electronically from the PIV card.
2. One or more of the CHUID data elements (FASC-N, Agency Code, Data Universal Number System) are used to determine whether the PIV cardholder should have access.
3. In addition, the following optional elements can be used:
 - The digital signature of the CHUID can be checked to ensure that it was signed by a trusted source and is unaltered.
 - The expiration date of the CHUID can be checked to ensure that the PIV card has not expired

4.7.2.3 Biometric Authentication

A PIV card contains, at a minimum, a digitally signed fingerprint biometric that can be used for authentication. The biometric data is stored only in a contact ICC. Therefore, only contact readers can be used for authentication purposes. However, the authentication can be unattended or attended.

Unattended biometric authentication takes place when there is no security guard or attendant at a physical access point. The PIV cardholder enters a PIN and provides a biometric without supervision. Because the cardholder could be providing their PIN and biometric under duress, unattended biometric authentication provides *high confidence* in the identity of the cardholder.

Attended biometric authentication takes place when there is a security guard or attendant at a physical access point. The PIV cardholder enters a PIN and provides a biometric under supervision. Attended biometric authentication provides very high confidence in the identity of the cardholder, because a security guard or attendant witnesses the transaction.

Federal Identity Management Handbook

Two biometric fingerprints are stored on a PIV card. Agencies can chose to use both fingerprints or only one for authentication purposes. FIPS 201 does not mandate where the match takes place: off the card (on a reader or server) or on the card.

4.7.2.3.1 Match Off the Card

1. The CHUID is read from the PIV card.
2. The expiration date of the CHUID is read to ensure that the PIV card is not expired.
3. The cardholder is prompted to enter a PIN. Entering the PIN activates the PIV card and allows a reader to check the biometric.
4. The PIV biometric is read from the PIV card.
5. The PIV cardholder is prompted to submit a biometric sample.
6. The sample is compared with the biometric. If the biometrics match, the cardholder is authenticated as the owner of the card.
7. The FASC-N in the CHUID is compared with the FASC-N in the signed attributes field of the external digital signature on the biometric.
8. One or more of the CHUID data elements ((FASC-N, Agency Code, Data Universal Number System) are used to determine whether the PIV cardholder should be granted access.
9. (Optional) The digital signature of the biometric is verified to ensure that the stored biometric is intact and comes from a trusted source.

4.7.2.3.2 Match On the Card

1. The CHUID is read from the PIV card.
2. The expiration date of the CHUID is read to ensure that the PIV card is not expired.
3. The cardholder is prompted to enter a PIN. Entering the PIN activates the PIV card.
4. The PIV cardholder is prompted to submit a biometric sample.
5. The sample is compared to the biometric stored on the card. If the biometrics matches, the cardholder is authenticated as the owner of the card.
6. The FASC-N in the CHUID is compared with the FASC-N in the signed attributes field of the external digital signature on the biometric.
7. One or more of the CHUID data elements (FASC-N, Agency Code, Data Universal Number System) are used to determine whether the PIV cardholder should be granted access.
8. (Optional) The digital signature of the biometric is verified to ensure that the stored biometric is intact and comes from a trusted source.

4.7.2.4 PKI Authentication

A PIV card carries mandatory and optional asymmetric private keys and corresponding certificates that can be used for authentication.

The process for using asymmetric cryptography is as follows:

1. The cardholder is prompted to enter a PIN. By entering the PIN, the cardholder activates the PIV card and allows a card reader to access it.
2. The card reader issues a challenge request to the card and requests an asymmetric operation in response.
3. The PIV card signs the challenge request with the PIV authentication private key and attaches the associated certificate.
4. The card reader verifies the response signature and PKI path validation is conducted in compliance with X.509 certificate policy. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure that the certificate has not been revoked.
5. The subject distinguished name and FASC-N are extracted from the authentication certificate and passed to the authorization function (this step requires connectivity to the PKI network. Stand-alone access control systems will not be able to perform this step).

4.7.3 Graduated Identity Assurance Levels

The authentication mechanisms described above can be used to provide graduated assurance levels for identity authentication. For example, electronic authentication mechanisms generally provide higher level of confidence in the identity of an individual than visual authentication mechanisms. Agencies may wish to combine authentication mechanisms to enhance the confidence in identity authentication.

The assurance levels are to be applied to both physical and logical access environments. Physical access environments include buildings and facilities. Logical access environments include personal computers, networks, and computer applications. Individual agencies are responsible for determining their physical and logical access control permissions, assigning assurance levels to their physical and logical assets, and implementing the authentication mechanisms discussed above.

Table 12 illustrates which authentication mechanisms can be implemented for the three PIV assurance levels for granting logical and physical access. The table depicts what mechanisms can be used but does not judge whether the authentication mechanisms are feasible for use in each access control environment. For example, it may not be feasible for a security official to watch individuals present their biometric for logical access, but agencies can do so if they wish. Additionally, an authentication mechanism used to ensure a higher level of assurance can be used to ensure a lower level of assurance. For example, any authentication mechanism that achieves *very high confidence* can also be applied to provide *high confidence* and *some confidence* in the assurance of an individual.

Table 12. Assurance Levels and Authentication Mechanisms for Physical and Logical Access

Assurance Level	Mechanism for Physical Access	Mechanism for Logical Access
Some confidence	Visual CHUID	CHUID PKI
High confidence	Unattended biometric	Unattended biometric PKI
Very high confidence	Attended biometric PKI	Attended biometric PKI

4.8 PIV II – Special Technical Publication 800-73

Place Holder

5. Implementation Planning

5.1 Acquisition Planning

The information in this section will help guide Federal agencies acquire the components and services needed to comply with HSPD-12 and FIPS 201.

FIPS 201 compliance is more than simply a requirement to purchase smart cards, hardware, and software. Compliance also represents an opportunity for agencies to assess and adjust their current business and operational processes to make them more efficient, secure, and consistent across the Federal Government. For example, every Federal agency supports an identity proofing and registration process for its employees and contractors. As part of this process, the prospective employee provides the agency with various forms of identification and, typically, a record of the prospect's fingerprints. The agency then typically processes a background check on the prospective employee. The agency's identity-proofing process constitutes the agency's *trust model*. The trust model is the basis for an agency's belief that the individual is the person the individual claims to be. The HSPD-12 control objectives are intended to establish a common, interoperable, and secure method for identification and a common trust model for use by all agencies within the Federal Government.

How an agency ultimately manages the acquisition process depends on factors such as the agency's size and the distribution of their facilities and personnel. Agencies should form centralized enterprise-wide acquisition capabilities for coordination of their PIV acquisition requirements. Centralizing acquisition provides agencies with the following benefits:

- Consolidated hardware and software requirements
- Acquisition of common, interoperable products
- Consistent warranty and maintenance programs
- Purchase discounts based on volume
- A consistent approach to solving common problems
- Better budget control

Figure 15 illustrates a typical agency organizational structure for PIV implementation. This structure includes business management and acquisition. The business management and acquisition functions should interact directly with the other implementation functions.

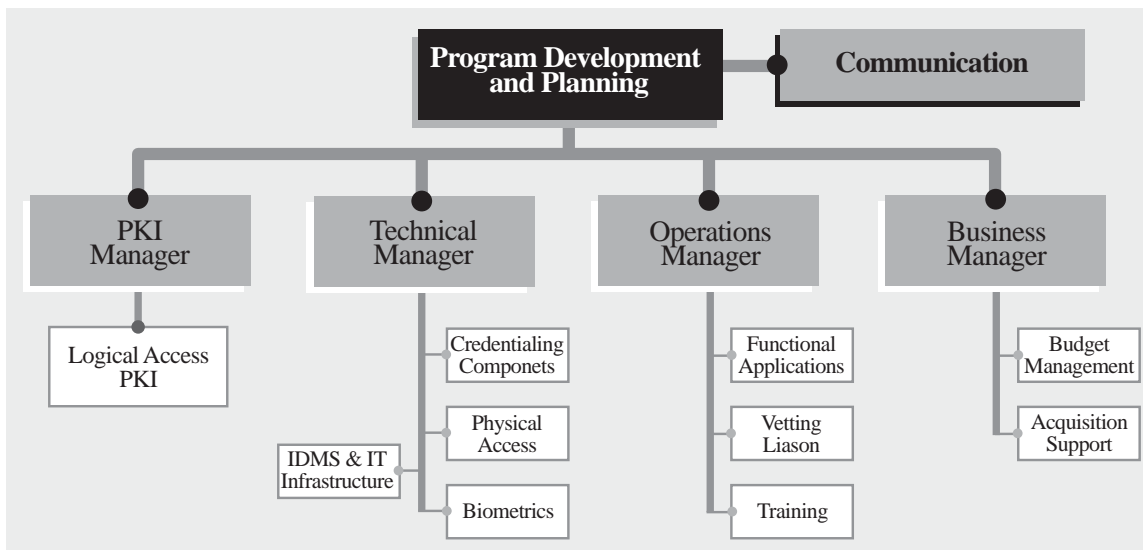


FIGURE 15. EXAMPLE ORGANIZATION STRUCTURE FOR AGENCIES PIV IMPLEMENTATION

5.1.1 Funding Streams

Whether funding is an issue for an agency will depend on whether the agency will need to acquire goods and services to comply with FIPS. Agencies should first evaluate their current business and operating processes to determine whether these processes already satisfy the requirements in FIPS 201. If not, it may be possible to meet these requirements by redesigning one or more processes. Agencies should consider implementation of FIPS 201 as the next logical step in evolving their identity management capabilities, not as a mandate to discard their current systems and start over. Although process redesign can be complex, it may not always require the purchase of goods or services.

When goods or services *are* required, an agency should consider several alternative funding streams. As an example, existing budgets should be reviewed to determine what level of funding is currently planned for upgrades to building security, personnel data management, and information technology security (i.e., in the agency’s current physical security, human resources, and logical security budgets). Funding may already be available in these areas to satisfy FIPS 201 requirements.

It is not possible to recommend a single acquisition solution that will work for every agency. Current identification systems and procedures will differ. Therefore, agency requirements for FIPS 201 compliance may vary. The specific quantities of goods and services required to meet the standard at each agency will be agency-specific. Once the funding sources are identified, an agency can conduct funds transfers between internal departments to the centralized acquisition team.

Table 13 lists some agency personnel who should be involved in the acquisition process.

Table 13. Potential FIPS 201 Acquisition Stakeholders

Function	CFO	Head of Security	CIO	HR
Physical security	X	X		
Logical	X		X	
Personnel	X			X

Change Management and Training

Proper training is critical to successful implementation. Every agency must ensure that everyone who is directly or indirectly part of the PIV process is trained. “Everyone” includes an agency’s management, PIV Sponsors, Registrars, Issuers, the Privacy Officer, and every approved Applicant for a PIV card.

Each role requires unique training. For example, a PIV cardholder should understand the proper use of the PIV card, its electronic capability, and how to keep the card secure. Standard, interactive web-based training programs and modules are planned for the PIV program. Following the completion of a training module, each trainee should be asked to complete a course evaluation and a test.

Agencies should regard training as a component of implementation cost. Per-user training costs will be conveyed as the training modules are completed. Table 14 indicates the approximate amount of time it will take to complete a specific training module.

Table 14. Amount of Time Required to Train PIV Roles

Role	Time to Train
Agency Management	60 minutes
PIV Applicant	15 minutes
PIV Sponsor	30 minutes
PIV Registrar	60 minutes
PIV Issuer	1 to 2 days

5.1.2 Current Methods of Procurement

5.1.2.1 GSA Smart Card Contract Vehicle

The GSA Smart Card Contract is available for use by all Federal agencies. The Smart Card Contract is a mechanism that can be used to issue smart cards for basic visual identification, identification authentication, physical and logical access control, cryptographic services, biometrics functions, and value-added features. It is recommended that agencies use GSA’s Smart Card Contract Vehicle. GSA’s Smart Card Program is a cooperative effort of GSA and the Common Access ID Steering Committee, composed of representatives from the Federal civilian, defense, and intelligence communities. The Smart Card Program allows Federal agencies and organizations to select from

Federal Identity Management Handbook

multiple vendors to meet their requirements. Under this contract, smart-card products and services are available to Federal agencies and organizations worldwide.

Qualified systems integrators compete to provide complete smart-card solutions. In addition to supplying the card and accompanying applications, a contractor may provide smart-card management services and smart-card system integration. One major advantage of using this acquisition method is that agencies can compare different technical solutions and costs for similar contract line items. Another is that the integrator takes responsibility for support and maintenance of the entire installed solution. Additional background information for GSA's Smart Card Program can be downloaded from www.fedcac.gsa.gov/smartcard.htm.

5.1.2.2 Individual GSA Schedules

When using GSA's Smart Card Contract Vehicle is impractical, agencies can use individual GSA Schedules. Using a schedule is recommended primarily to acquire quick turn-around for commodity or consumable item acquisitions. This method is not recommended when support or a warranty is required, or if the item being procured could affect the functionality of the infrastructure.

GSA Aggregated Buy. GSA's Aggregated Buy is a program developed by a coalition of Federal agencies in conjunction with GSA to leverage the buying power of the Federal Government. The program is designed to pool the requirements of participating agencies for certain high-volume items such as smart-card stock.

Aggregated Buys are planned to occur on a quarterly basis. The first quarterly aggregated buy is planned for mid-April 2005. It is currently anticipated that the program will be used to make regular quarterly buys of smart cards, providing participating agencies with quantity discounts. In the future, middleware, card printing consumables, and PC/SC smart card readers for logical access will be added to the program.

To facilitate this process, participating agencies will provide their purchase requirements and associated funding to a representative of GSA's Office of Smart Cards (FTS). Agencies wishing to participate in a quarterly aggregated buy should complete the following steps prior to the beginning of the next fiscal quarter. (As an example, for participation in an April buy, all planning steps should be completed before the second week in March.) The steps are:

- Determine which contract line items and how much of each your organization needs. If assistance is needed in determining your agency's requirements, contact the GSA Smart Card Office at 202/208-3055.
- Prepare a funding document (MIPR, P.O., RWA) and forward it to GSA/TFS, Rm.5010, 1800 F Street, NW, Washington, DC 20450. Documents can also be faxed to 202/208-3133. Mark the document "For Project # 24612INS."

5.1.3 Major Components of an Identity-Management System

Implementation of a fully functional identity-management system can represent a significant and complex effort requiring the coordination of many resources. Figure 16 illustrates a high-level view of the major components of an identity management infrastructure to assist agencies in understanding the potential extent of an integration effort.

Federal Identity Management Handbook

Identity Management Process	Potential Asset/Resources Required	Identity Management Process	Potential Asset/Resources Required
<p>PIV Identity Proofing & Registration</p> <p><i>Note:</i> can be centralized or distributed</p>	<ul style="list-style-type: none"> • Identity Source Documents • Biometric Capture Device • Source Document Scanner • Background Investigation (NACI, NACiC, LBI/BI) • Program Management • Systems Integration 	<p>PIV Card Revocation</p>	<ul style="list-style-type: none"> • Identity Management System (HW/SW) • License Fees • Maintenance • Program Management • Systems Integration
<p>PIV Enrollment</p> <p><i>Note:</i> can be centralized or distributed</p>	<ul style="list-style-type: none"> • Data Capture HW/SW • Computer, Monitor, Keyboard • Biometric capture Device • PIN Pad • Camera • ID card Printer & Printing Consumables • Test Reader • Card reader/writer • Program Management • Systems Integration • System Maintenance Fees 	<p>Card Management</p>	<ul style="list-style-type: none"> • Card Management System (HW/SW) • Software License Fees • System Maintenance Fees • Program Management • Systems Integration
<p>Cryptographic Key Management</p>	<ul style="list-style-type: none"> • Hardware Security Modules • Key Management System (HW/SW) • PKI • Program Management • Systems Integration 	<p>Card Issuance</p> <p><i>Note:</i> can be centralized or distributed</p>	<ul style="list-style-type: none"> • Card Issuance System (HW/SW) • Software License Fees • System Maintenance Fees • Program Management • Systems Integration
<p>Smart Card Stock</p>	<ul style="list-style-type: none"> • Applets • File Containers • Smart Card Initialization Software • Licensing fee for software • Program Management • Systems Integration 	<p>Physical Access Control</p>	<ul style="list-style-type: none"> • Smart Card Readers/biometric readers/PIN Pad • Access Control Panels/IP Device • Wiring and Fiber Optics • Door Locking Hardware • Turnstiles
		<p>Logical Access Control</p>	<ul style="list-style-type: none"> • Smart Card Readers • Biometric Readers

FIGURE 16. IDENTITY MANAGEMENT COMPONENTS AND EXAMPLES OF THE ASSETS REQUIRED

5.1.4 Anticipating Implementation Costs

Various factors can contribute to an agency’s overall cost. PIV applicant volume, (anticipated number of future employees and contractors to join the agency) and potential cost sharing within and among agencies are also factors. Because vendors offer sliding scales for pricing on products and services, agencies can coordinate their procurements to obtain discounts.

Agencies can also save costs through consolidation. One of the most compelling business cases for the use of smart cards is the potential cost savings resulting from implementing several applications on one platform. Agencies can also consolidate functions, creating economies of scale that lead to reduced costs in areas such as card issuance and administration. Additionally, card issuers and application owners are expected to benefit from reduced costs due to sharing the following services:

- **Core Services.** Data processing that supports core services is shared among all programs using card applications.
- **Data Collection.** The costs of gathering and storing common data are shared among application owners.

Federal Identity Management Handbook

- **Card Personalization.** The PIV is personalized and issued once, rather than once per application.
- **Infrastructure.** For many applications, infrastructure can be shared among application owners.

The investment required to upgrade the infrastructure and transition to a smart-card platform consists of costs for design and development and costs for implementation. Design and development costs are commonly incurred by the following:

- Detailed system design and review
- Hardware and software development
- System demonstration and acceptance testing
- Training and documentation
- Project administration
- Smart card reissue percentage
- Data sharing/data interface costs
- Independent validation and verification

Implementing a fully functional smart-card infrastructure requires more than simply printing and issuing smart cards. A complete smart-card implementation can be a complex program management task. First and foremost, the agency should define its functional and technical requirements based on their physical and logical access requirements.

5.1.4.1 Anticipating Costs of Smart-Card Related Equipment

A wide variety of equipment is currently available in the commercial marketplace to assist with the identity management process. New models and technologies are introduced seemingly on a daily basis. Although it is not possible to present a complete list of all products on the market or specific models and pricing, it is necessary to recognize that different technologies and price points exist to satisfy a similar need. It is important, therefore, to assess the long-term logistical requirements before making a purchase decision.

A product conformance testing suite is planned for FIPS 201 related products. Vendors can, at their cost, submit products for testing and, if the products pass, add them to an approved products list for FIPS 201. Prior to procurement, agencies should conduct their own interoperability test on approved products. (For more information, see Section 5.5.).

Table 15 lists various items that may be useful for a successful FIPS 201 implementation. Although the list is by no means exhaustive, it indicates what types of smart card and related hardware and software are currently available and their relative cost. Volume discounts are not incorporated into this table.

There are often several ways to satisfy a single requirement. Agency acquisition teams should select combinations of products and services that are appropriate for their implementation.

Federal Identity Management Handbook

Table 15. Sample Smart-Card Related Products List

Item	Description	Use	Unit Price
Smart-card token	Credentialing device with a contact and contactless interface	Physical and logical access control applications	\$5 - \$15
Contact smart card reader (USB)	Device for reading the information stored on the smart-card token through a contact interface	Logical access for secure access to computer systems	\$15 - \$25
Contactless smart card reader	Device for reading the information stored on the smart-card token through a contactless interface	Physical access for secure access to secure buildings and facilities	\$300 - \$1,500
PC keyboard smart card reader	PC Smart Card Reader for reading the information stored on the smart-card contact interface	Logical access	\$15 - \$50
Fingerprint reader/scanner	Fingerprint biometric acquisition device	Physical and logical access control applications	\$25 - \$125
Document scanner	Device used to read documents presented for identification	Provide a level of assurance that a document presented to verify identity are not forged or manipulated	Cost may vary significantly
ID card printer, low volume	Desktop smart card printer	Card printing	\$1,000 - \$4,000
ID card printer, high volume	Large batch smart card printer	Card printing	\$6,000 - \$12,000
Smart card middleware	Software that enables the card to communicate with the reader	Logical access	\$2 - \$10 per seat
Smart card management system	Supports issuance and lifecycle management of smart cards and data stored on the cards	Maintenance and support	\$5 - \$50 per seat
Centralized smart card personalization	Completing the topographical printing and ICC initialization at a secure central facility vice multiple locations	PIV production and issuance	\$3 - \$5 per smart card

5.1.5 Agency PIV Sponsorship

Some Federal agencies may find it impractical to implement PIV identification on their own. The concept of agency PIV sponsorship was developed to help such agencies. Agency PIV sponsorship enables an agency that has successfully implemented a smart-card identification program to help another agency become FIPS 201 compliant by providing smart-card services. Entering into this type of arrangement does not relieve the sponsored agency of compliance responsibility, but it may offer the sponsored agency significant advantages, including reduced costs.

A sponsoring agency can provide services such as PIV registration, personalization, issuance, data management, and card management. Sponsored agencies cannot transfer responsibility for implementing the following PIV roles and functions:

- Applicant sponsorship
- Applicant pre-enrollment, enrollment
- Completion of PIV application
- Collection and verification of identification forms
- PIV approval and authorization
- PIV card stock acquisition (agency specific security keys)
- PIV card visual design

The services a sponsoring agency may provide include:

- PIV card production
- Card issuance
- Card activation
- Card maintenance

The sponsored and the sponsoring agencies can share the following responsibilities:

- ID vetting (registration)
- Data management
- PKI

Additional information on agency sponsorship is available at www.fedcac.gsa.gov/smartcard.htm.

5.1.6 Shared Service Provider

The Shared Service Provider (SSP) program is operated by the FICC. The purpose of the program is to ensure that third-party PKI service vendors can satisfy the U.S. Government requirements for issuing and managing medium assurance (and higher) digital certificates on smart card tokens that satisfy all the requirements of the U.S. Common Policy Framework, FIPS 201 and NIST SP 800-73. Vendors who successfully pass these policy, procedural, and operational requirements are added to the Certified Providers List and their certificates express the Common Policy OIDs. SSP vendors' CAs are cross-certified with the Federal Bridge CA (FBCA) through the Common Policy linkage.

Federal Identity Management Handbook

After December 2005, Federal entities newly implementing PKIs will be required to get their certificates and services through the SSP program unless explicitly exempted by OMB.

5.1.6.1 Federal Legislation

Section 210 of the Electronic Government Act of 2002 authorizes agencies to enter into share-in-savings contracts, whereby agencies can consolidate their information technology purchases to reduce overall operating expenses and improve efficiency. Applying the guidance provided in this policy, OMB has decided that, beginning in 2006, agencies will procure PKI equipment and services through qualified service providers. The purpose of this mandate is to endorse a uniform implementation policy and enhance the interoperability of public key infrastructures across the Federal enterprise.

The SSP Working Group was commissioned to evaluate PKI vendor compliance with the PKI Common Policy and facilitate the PKI implementation process for Federal agencies. On March 11, 2004, a conference was held to introduce the SSP Working Group's goals to industry representatives and outline the certification process. Following an application process that included demonstration of vendor PKI capabilities and compliance with Federal technical specifications, an initial Qualified Bidders List was published on June 30, 2004. Currently, new applications are being accepted from PKI vendors who want to be added to the Certified Providers List. The Certified Providers List and all supporting documentation for SSP applicants is available at <http://www.cio.gov/ficc/>.

5.1.6.2 A Common Policy

The SSP Working Group is specifically tasked with ensuring that qualified vendors can issue medium or higher digital certificates to Federal employees, contractors, and third-party affiliates. The primary SSP Working Group activity has been to establish a pool of qualified PKI vendors, complementing the government policy mandating the implementation of an agency PKI system under the Federal Common Policy root certification authority. As agencies issue contracts to qualified service providers, all agency PKI architectures will have a similar design and agencies will more easily be able to trust each other's digital certificates.

The publication of an SSP Certified Providers List also helps further the development and adoption of government-wide standards for electronic identity management using PKI technology. The current standard for cryptographic modules for logical access is *Security Requirements for Cryptographic Modules*. The Federal Government created this standard for use in agency PKI applications. Documents such as the SSP Certified Providers List reinforces the government's requirement for standards. As standards continue to evolve and a greater number of vendors comply with them, PKI certificate interoperability will be extended across the Federal enterprise.

The SSP Certified Providers List lists vendors that meet the criteria of the Common Policy Framework. Government agencies can consult the list to find an appropriate vendor and to procure PKI products and services through a GSA Schedule 70 Contract. Companies that are already providing PKI services to the government under other contract mechanisms are not required to change their contracts, however, only by successfully completing the SSP suite of tests can a vendor be a Certified SSP Provider of PKI services.

5.1.6.3 Agency Requirements

The SSP program enables agencies to outsource their PKI-related services to a pre-qualified vendor. This opportunity may make an especially strong business case for smaller agencies that are unable to meet the staffing and operational requirements of a PKI system by themselves. However, agencies must comply with a few requirements even when they partner with a service provider. These requirements are introduced below.

5.1.6.4 Certification and Accreditation

Federal regulations mandate that agencies complete the certification and accreditation process for SSPs. To help agencies comply with this requirement, the SSP Working Group requires the SSP applicant to complete a security certification and accreditation assessment on the government's behalf. This process helps contracting agencies mitigate the risks associated with introducing new information technology systems into their existing operations. Guidelines for completing the assessment are defined in SP 800-37. The SSP applicant incurs the cost of the assessment.

Figure 17 illustrates the four primary components of the certification and accreditation process and details the major tasks associated with each component.

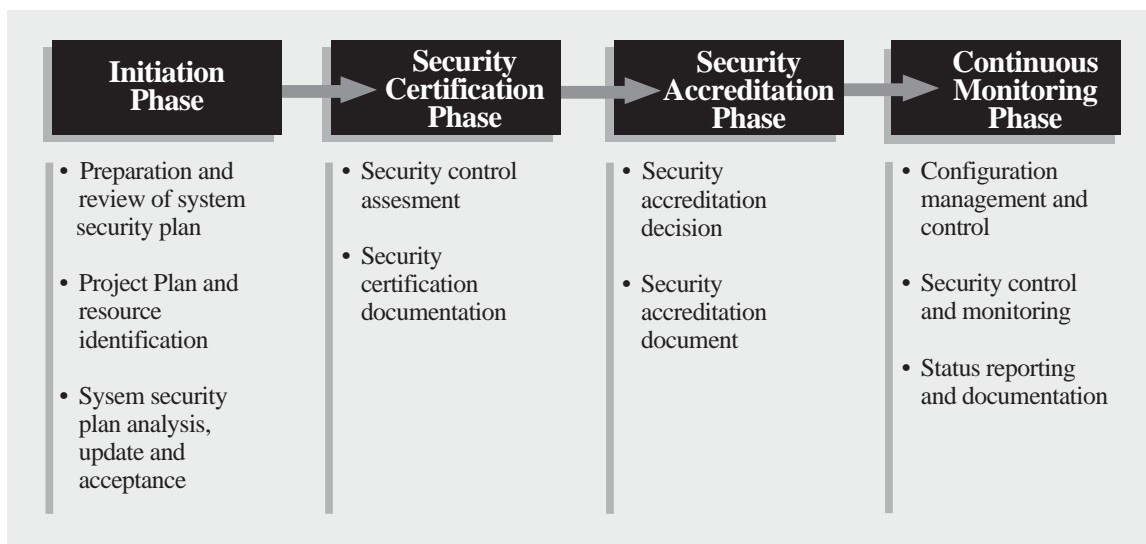


FIGURE 17. FOUR PRIMARY COMPONENTS OF SSP CERTIFICATION AND ACCREDITATION PROCESS

Completion of this process results in a unique certification and accreditation report that agencies can reference. As agencies prepare to implement PKI systems, they can leverage the work already completed by the SSP applicants, fulfill their Federal regulatory requirement for completing the certification and accreditation process, and reduce their initial PKI system investment.

While an agency can take advantage of the certification and accreditation assessment conducted by a service provider, it is still required to complete its own certification and accreditation assessment of the identity-proofing process it uses to issue identity credentials. An RA under agency control is responsible for identity-proofing each user. While an agency may choose to outsource RA functions to

Federal Identity Management Handbook

a qualified service provider, it must retain authority for, and responsibility for local certificate issuance decision-making.

5.1.6.5 The Post-Acceptance Process

Federal policy requires that each agency perform a periodic certification and accreditation evaluation of its identity-proofing process. This evaluation should focus specifically on the RA's role in identity-proofing candidates for digital certificates. The certification and accreditation process must be repeated every 3 years, or whenever the system undergoes a major modification. The renewal of the certification and accreditation report is in accordance with OMB A-130.⁴⁸

5.1.6.6 Agency Archive Requirement

Each agency is responsible for developing and implementing a records management plan that will meet the agency's regulatory, legal, and business needs as well as the SSP archive requirements. Archive requirements are documented in the *X.509 Certificate Policy for the Common Policy Framework*, section 4.6, "Records Archival." In this context, "archival" refers to the management of records for an unlimited period of time in a location that is physically separate from the CA or RA that initially generated the record. General guidance for management of such records for Federal Agency use is published in *Records Management Guidance For PKI-Unique Administrative Records*. This guidance is available at two locations:

http://www.archives.gov/records_management/policy_and_guidance/pki_guidance.html

<http://www.cio.gov/fpkisc/library.htm>

The completed records management plan and an accompanying SF-115 form are submitted to the National Archives and Records Administration for approval. The agency must ensure that its SSP can execute all tasks documented in the plan.

5.1.7 Acquisition Planning Template

Agencies should allow sufficient time to plan for each step of their employee identification project. It is therefore essential for agencies to have a clear understanding of the government's PIV compliance milestones. Agencies requiring clarification should refer to OMB implementation guidance and the National Institute for Standards and Technology (NIST).

A sample acquisition planning template is provided in Appendix to assist agencies with PIV budget planning. The requirement for preparation of the written acquisition plan is defined in the *Federal Acquisition Regulation (FAR) Part 7* (as supplemented by the *General Services Administration Manual*, Part 507). This template is not intended to substitute for these regulations, but rather to assist in preparation of an acquisition plan.

⁴⁸ Office of Management and Budget Circular No. A-130.

5.2 Migration Planning

Federal agency identity credentialing systems are currently integrated to different levels of completion. Once agencies understand FIPS 201 requirements, they will need to evaluate their current credentialing environment to determine how to comply with the mandated requirements. The agency's credentialing program and business practices may then need to be modified to comply with the new standard.

This section provides practical guidance on how to conduct this process. The section consolidates identity management best practices and functional process guidelines. As agencies migrate toward FIPS 201 compliance, they will also want to reference two documents: HSPD-12 and the OMB HSPD-12 Implementation Guidance.⁴⁹

5.2.1 HSPD-12 Guidance

HSPD-12 defines control objectives that are critical to implementation of a common, interoperable Federal identification credential. The goal of HSPD-12 and FIPS 201 is to provide the framework and specifications for a commonly accepted, interoperable, secure identity credential based on sound and accepted identity-proofing procedures. Specific physical and logical access decisions are under the control of the agencies. Individual agencies should determine what levels of assurance are required for physical and logical access points.

5.2.2 OMB Implementation Guidance

OMB's Implementation Guidance identifies milestones that Federal agencies must meet as they implement the new credentialing requirements. A timeline is provided for the delivery of the Agency Implementation Plan and a separate document that identifies facilities, systems, and other applications that are important for security but not covered in HSPD-12. A schedule is also provided for FIPS 201 PIV I and PIV II implementation.

5.2.3 Key Benefits of Business and Systems Integration

A Federal agency can realize numerous tangible benefits from deploying a federated credential. A robust authentication process based on credentialing technology can enhance security and create detailed audit trails while increasing protection for employee privacy rights. Ultimately, the impact of these benefits will be strongest when agencies are able to integrate their building security applications with their network security applications. In most cases, such integration is still in the future. However, it is worthwhile to consider such an architecture.

In recent years, human resources, physical security, and information security have begun to require and use the same data. Smart cards are already capable of communicating with physical and logical access control applications. If the back-end databases that support the applications could be integrated, an agency could benefit from consolidated security management, faster response rates, improved detection and audit control, and uniform policies. Furthermore, the convergence of PIV cardholder information is supported by the emergence of a standardized PIV card that will encourage interoperability and file sharing. A fully integrated system can immediately reflect an employee's status, including changes resulting from hiring, termination, or altered access privileges.

⁴⁹ Office of Management and Budget, *FIPS 201 Implementation Guidance*.

Federal Identity Management Handbook

Human resources, physical security, and information security departments can retain their autonomy and still integrate their data by maintaining a common centralized identity management network. The databases could be partitioned and the network might manage only the PIV cardholder data elements that are required for access control; the remaining files for a cardholder, such as background check results and digital certificates, could be managed from a back-end database by the appropriate agency department. The information sent to the network could not be rerouted to another department's network. Figure 18 illustrates one possible architecture in which three otherwise autonomous departments consolidate their PIV cardholder information in a central identity-management system.

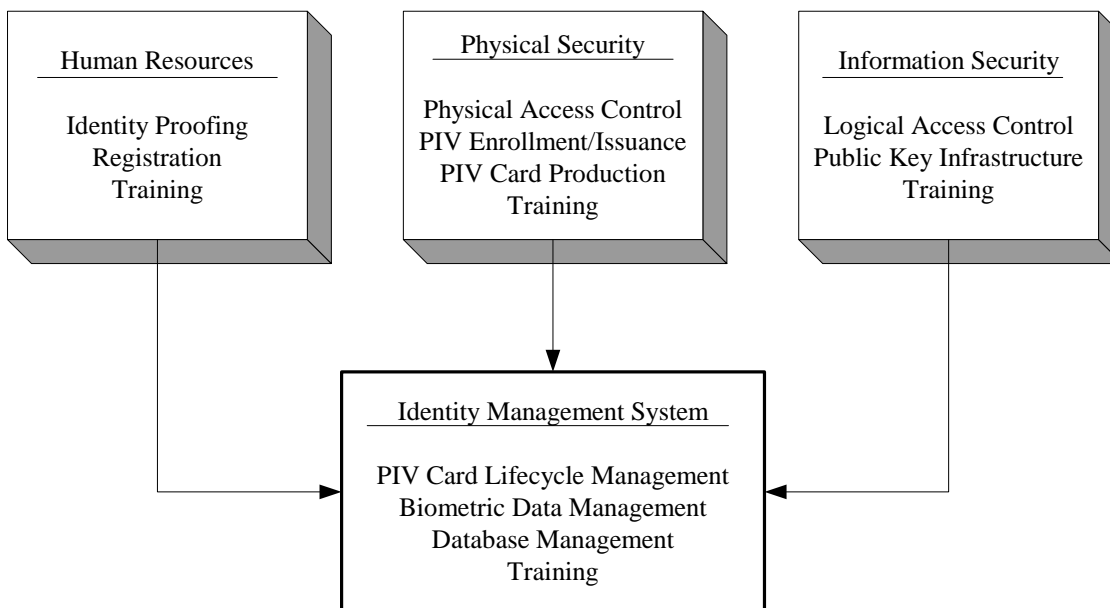


FIGURE 18. IDENTITY MANAGEMENT CONVERGENCE ARCHITECTURE

Many choices are available to an agency, and the final decision will be influenced by security requirements, business needs, budgets, legacy systems, and other determining factors. Given the wide selection of available security products and the many combinations in which they can be integrated, it is easy to imagine the high degree of customization that an agency may require. To facilitate the migration process, specific variables are identified here that agencies should consider when comparing their requirements with products and solutions providers.

A Federal agency's success at managing its security requirements is contingent upon its processes for auditing governance, compliance, and use. Because many different users access an agency's facilities and networks, it is especially challenging for an agency to grant the necessary rights and privileges to each user while still protecting the confidentiality and privacy of its users and data. An effective credentialing methodology represents the key driver for agency security.

5.2.4 Developing the Migration Plan

The transition to the multi-application card platform required to comply with FIPS 201 may be transformational for many agencies. Several years may have passed since an agency designed its current identity management system. During this time, technology and standards have evolved, and

Federal Identity Management Handbook

discrepancies may exist between the current state of technology, current implementation standards, and an agency's current system.

A migration plan defines a critical path to FIPS 201 compliance that accommodates all dependencies of the PIV system. The plan evaluates the tasks, dependencies, resources, and milestones required for deployment of the PIV card. A proficient migration plan explains how to resolve discrepancies between the current identity management system and a FIPS 201-compliant system. It also describes how to mitigate transitional vulnerabilities. Key stakeholders in an agency, including information technology, physical security, and human resources administrators, should use the migration plan to structure and implement the transition to a FIPS 201-compliant system.

FIPS 201 introduces some new credentialing concepts that may be unfamiliar to agencies. The transition to this new credentialing environment will require many decisions. A proficient migration plan defines a standardized process for re-engineering current security applications or business processes that is based on consistent, feasible, and documented decisions. After such a plan is implemented and the replacement policies are in place, an agency will immediately be able to take advantage of a new PIV system that reduces support costs, upgrades legacy technologies, and supports a common Federal credentialing environment.

While it is not possible for this handbook to propose a migration plan that is appropriate for every agency, migration to a FIPS 201-compliant system includes a number of processes and requirements common to all agencies. These common processes and requirements are discussed in the following sections. Agencies are encouraged to use this guidance as a template, customize it as needed, and rely on it as a road map to FIPS 201 compliance. Figure 19 illustrates a suggested FIPS 201 migration-plan road map.

Federal Identity Management Handbook

defines a schedule for PIV system deployment. A Roadmap Plan should consolidate the requirements from both of these documents and provide the agency with a single reference document for achieving compliance.

- **Statement of Work.** The statement of work provides a conceptual definition of the migration process. The statement of work is composed of major business drivers and a project work plan.
- **Gather Process Documentation.** Referencing FIPS 201 and its accompanying technical Special Publications, compare the PIV system requirements with the legacy system requirements.
- **Review Availability of Funds.** The FIPS 201 implementation timeline may be shorter than the agency's procurement cycles. Successful migration will require agencies to simultaneously reallocate funds and plan their process re-engineering efforts. A PIV system should be considered an extension of the agency's existing credentialing system, not a new program.

5.2.4.2 Validate Solution

In the Validate Solution stage, the assumptions derived in the Prepare stage are validated, using empirical evidence and experience that the agency has acquired by using its current credentialing system. In this stage, an agency will need to determine whether the PIV system architecture it has designed meets all the requirements of FIPS 201.

To accomplish this, an agency should review the results of conformance testing for potential interoperability issues between different PIV system components such as cards, readers, and biometric acquisition devices. Conformance testing will also validate specific vendor product certifications.

Another tool that can be used to validate a proposed PIV solution is the planned NIST FIPS 201 Reference Implementation. Once the Reference Implementation is available, it will be able to partially alleviate an agency's obligation to test whether a particular vendor's card is compatible with the SP 800-73 specifications. Instead, agencies can simply require that PIV vendor products (such as client applications and middleware) perform satisfactorily against the Reference Implementation.

Additional activities that should be completed during this stage include:

- **Complete Agency Plan.** The Agency Plan enables an agency to correlate its current identity management policies with the HSPD-12 control objectives. This template will provide agencies with significant insight into the PIV migration process.
- **Submit HSPD-12 Agency Plan to OMB for Approval.** The Agency Plan is submitted to OMB for review and approval. This review process offers agencies an unbiased and objective perspective on issues relevant to their credentialing system.

5.2.4.3 Design, Develop, and Test

Once the PIV implementation solution is validated, the Design, Develop, and Test stage can begin. In this stage, the system architectural design is reviewed and tuned.

Federal Identity Management Handbook

An agency should consider how PIV-related data is used throughout the PIV system. The level of data redundancy between the legacy and PIV system should be evaluated. For example, it should be determined whether data files from the legacy system will be applicable to the PIV system. It is likely that they will, and these files should be absorbed into the PIV system. Similarly, if there are discrepancies in the data field names between the legacy and PIV system, a design modification should be made to ensure consistent naming conventions. For example, it should be noted whether user field names are composed of first and last names instead of eight characters.

Other questions that should be resolved include how users will access data during the migration process, what the data archiving requirements and reporting requirements for PIV card applications are, and whether hardware and software upgrades are required.

The following activities should also be completed during this stage:

- **Technical Solution and Business Policy Alignment.** As the technical infrastructure team refines the system architecture, the migration team should be finalizing the PIV system's business processes. One document that will facilitate this task is the HSPD-12 Agency Plan, which is included in Section 1.3.3 of this handbook for agencies to complete and submit to OMB. Completing the HSPD-12 Agency Plan provides agencies with an objective observer capable of assessing the viability of their migration plans.
- **Security Accreditation.** FIPS 201 also mandates the completion of a security accreditation process. PIV validation, certification, and accreditation is a quality assurance process that defines, evaluates, and certifies risk for a PIV system. Completion of this process is critical to identifying the operational and technical risks associated with a PIV system and certifying that the system is ready for deployment. For further information, refer to Section 3.0 of this handbook.

5.2.4.4 Train and Deploy

After successful completion of the three previous stages, an agency can confidently deploy its PIV system. Throughout this stage, predetermined performance metrics will be monitored so that system deployment can be evaluated properly. Business processes should ensure that detailed user procedures are available and incorporated into end-user training modules, so that all PIV card users are aware of how to use the card. Reporting tools should be established to track the system's performance and create reports. Finally, a robust test should be conducted on the system to determine whether it meets FIPS 201 and agency requirements.

The following represent additional activities to be completed during this stage:

- **Execute Communications Plan.** The Communications Plan that was drafted in the Prepare stage is deployed to provide hands-on support to all user groups.
- **Implement Training for Stakeholders.** Key stakeholders not involved with program management of the migration planning process will need to gain a working knowledge of the PIV system.
- **Update Risk Analysis and Mitigation Plan.** The Risk Analysis and Mitigation Plan should be considered a living document throughout the migration process, with frequent evaluations and modifications made based on the PIV system implementation.

5.2.4.5 Transition and Control

The Transition and Control stage represents the final stage of the migration process and the beginning of the PIV system's production phase. By this time, most of the system's process and technical issues should be resolved. Administrative roles associated with the migration plan are phased out and PIV program management roles are introduced. These roles may or may not be assigned to the same people.

It is recommended that best practices and lessons learned from the migration process be documented for future reference. This documentation, a user acceptance review, and the system's performance reports should be evaluated in a post-implementation review that will provide the agency with suggestions for continuously improving the PIV system.

After PIV cards are issued, it is the agency's responsibility to supervise the proper use of each card. It is very important for the integrity of the access control system that each individual access only those facilities and workstations that are authorized for that person's use. Supervision of access control can be accomplished with access control software that creates detailed audit trail logs. These reports provide access control system administrators with information on who is accessing specific applications.

5.3 Lessons Learned

This section highlights the lessons learned from interviews conducted with FICC Working Group chairpersons and Federal agency credentialing program managers. While the scope and scale of credentialing projects within the government vary widely, the observations made by those who participated in implementing and operating credentialing systems shared many commonalities. These comments are consolidated below.

5.3.1 Implementation Management

It is a best practice to limit the number of technologies or media on a smart card. A large number of collocated technologies increases both the likelihood of malfunction and the complexity of card lifecycle management. For example, a credential carrying both a magnetic stripe and a chip can be bent accidentally, and while the magnetic stripe can still be read, the chip is damaged or broken. Printing cards that carry multiple technologies has a higher degree of failure, because the printer must add each technology to the card perfectly. The variance in lifecycles for each technology can cause some of the technologies on the credential to be retired prematurely.

The use of credentialing tokens—and particularly smart cards—offers a dynamic solution for agencies that use only one or two card technologies today but will need to add other applications that are supported by the smart card ICC in the future. The versatility of a smart card makes this scenario feasible. With increases in memory capacity apparent in new generations of smart cards, an agency can purchase an advanced credential such as a smart card today and add applications over time. Doing so stretches the card's life over a number of years.

5.3.2 Stakeholder Management

Two requirements seem to be the most critical to the success of a standardized Federal credentialing program: enforcement of a single credentialing policy and the ability of Federal agencies to obtain the funding required to implement the policy. Federal agency project managers can be assured that both of these criteria are being resolved.

Federal credentialing policy has been consolidated in FIPS 201, which incorporates much of the work that has been completed by the FICC, the FICC working groups, the IAB, and the individual agencies.

Each agency is required to allocate funding to support the implementation of the new standard. The issuance of HSPD-12 requires project managers to procure and implement smart card technology. Previously, individual agencies could implement smart card technology at their own discretion.

As agency project managers prepare to implement the new standard, they should maintain communication with senior management, such as agency CIOs, physical access directors, and human resources executives. Buy-in and the active participation of leadership is important to the success of a credentialing program.

It is recommended that agency project managers inform their senior management of pending standards and legislative mandates that will influence the decision-making process. Moreover, it should be anticipated that some senior executives might not be familiar with credentialing technologies. Agency project managers should be prepared to educate them so that these executives can become more familiar with smart card technology. To meet this need, training modules for agency executives may become available that will underscore the importance of their participation in the PIV system business decisions. All stakeholders should be made aware that a properly implemented credentialing program represents a long-term investment that can enhance security and user convenience while reducing costs.

5.3.3 Procurement Plan

Once agencies have identified their credentialing requirements, the next logical step is to create a procurement plan. A procurement plan helps an agency select an optimal credentialing technology platform that will satisfy the agency's requirements while supporting future technology upgrades. To create a procurement plan, an agency should first conduct a thorough review of access control policies established by FIPS 201 and the agency's internal directives. This review will then inform the agency of the technical and functional requirements of a PIV system. This endeavor can only be successful if the cost of procuring the technology falls within the agency's budget.

Many individuals do not have accurate information about the cost of credentialing technology. For instance, one popular misconception is that smart cards contribute the majority of an implementation's costs. Smart cards actually represent a small fraction of total costs; the card management system, card readers, administration, support, maintenance, and other changes to the IT infrastructure to support new identity management processes comprise most of the costs. Agencies need accurate cost estimates to balance the costs and benefits of different credentialing technologies.

The Federal Government provides different resources for agency use in procuring new credentialing technologies. For example, use of the SSP Qualified Bidders List can facilitate an agency's PKI procurement process. A Federally sponsored aggregate card buy in December 2004 consolidated smart card purchases from many agencies, substantially reducing the price per card. The Federal government

will continue to support initiatives such as these by identifying common credentialing criteria and introducing programs that are designed to reduce costs for everyone.

5.3.4 System Design

The correct identification of credentialing requirements is critical to the success of an agency's credentialing program. To ensure that this process is conducted effectively, the agency needs to query users at all levels to determine exactly how they are using their credentials for access. There are many ways to collect this data, but questionnaires, interviews, and meetings are proven, low-cost methods that enable an agency to assess its requirements quickly.

Agencies with large-scale identity management systems have observed that the management of the credentialing system is more straightforward if the smart card is used as an authentication token only, not as a data storage device. In a typical work environment, the user authenticates to the agency network and accesses data directly from the network. No data other than the card personalization data used for identification management is stored on the card. This approach has three benefits:

- The most current information is available to the cardholder.
- The lack of ancillary data on the card allows an agency to prolong the card's life, because the card's memory requirements remain constant.
- The lack of ancillary data lowers an agency's operational risk. If the credential is compromised, there is no danger that sensitive information will be divulged.

5.3.5 System Interoperability

Although vendors are striving to comply with interoperability specifications such as GSC-IS and FIPS 201, the resolution of credential, reader, and chip interoperability issues will not automatically mean that agency security applications will operate seamlessly for an indefinite period of time.

Hardware components such as tokens, readers, and chips are technologically stable; because they have a long product lifecycle, they will not require frequent modifications or updates. However, technologies and applications such as card middleware, which includes applets, and card capability containers change more frequently. For example, altering the data model for a smart card could require updating the card middleware. This relatively common occurrence requires an agency to change each instance of the middleware. Because middleware is sometimes installed on individual workstations, this process can be inefficient.

5.3.6 Pilot and Production

Pilots and prototypes represent a valuable opportunity to evaluate a security application with a controlled amount of risk. Data derived from a pilot can be used to anticipate the results of full-scale production of the same system and to troubleshoot any difficulties that may arise.

If a pilot is carefully organized so that it involves a microcosm of the entire user community, an agency can learn from a pilot and modify the system before production.

5.3.7 Post-Operational Processes

Post-operational processes are critical to credentialing systems. Such processes can establish benchmarks for monitoring the system's use. The following resources can be integrated into a post-operational process:

- Logistic support that orders cards and consumable products when inventory falls beneath an established threshold
- Help desk for troubleshooting technical issues
- System administration tools that offer auditing, searching, and reporting functionality
- Card-management applications that can upgrade, reissue, and revoke credentials

5.3.8 Training

Interviews conducted with government credentialing experts indicate that credentialing project managers and issuing authorities assume users will understand how to use a credential quickly, with little or no training. Actually, users frequently are unaware of what applications are on the credential or how to use it properly. Moreover, they lack the authority to request training. Agencies can therefore anticipate a variable user acceptance rate.

To meet this challenge, agencies should develop and supervise a thorough training program. Such a program will assure agencies that its users are in fact using the PIV card for its intended purpose and users will recognize the importance of the PIV system to the agency.

5.4 Case Studies

Federal agencies are currently issuing many diverse forms of ID cards to enable employees and contractors to access government buildings and computer networks. The ease with which older generations of cards can be duplicated and the error factor inherent in humans scanning older cards at building entrances have led a number of agencies to adopt smart card technology. Smart card technology provides a more secure card, guards against identity theft, and fosters secure logical and physical access.

This section introduces current Federal smart card credentialing system case studies. There are a variety of smart card deployments in different development stages, and a variety of applications are supported by each deployment. This section also provides specific case studies related to smart card implementations at the Department of State, Department of Interior, and Transportation Security Administration.

The United States Government Accountability Office (GAO) completed a study on smart card technology in September 2004. The study reported on the agencies implementing this technology and the progress of each initiative. According to the GAO's report to Congress, *Federal Agencies Continue to Invest in Smart Card Technology*, GAO found that while Federal agencies are continuing to invest in this technology, more than half of these efforts have been discontinued. Two primary reasons were cited for discontinuation:

- Many projects have been "absorbed" by the larger scale smart card implementation efforts.

Federal Identity Management Handbook

- The remaining projects were deemed “no longer feasible.”

GAO’s findings state that only 24 of the 52 smart card technology initiatives started by various agencies are ongoing. Of these 24 projects, 16 are in the pilot, planning, or operational phase and are intended to support a variety of uses. (Information on the remaining eight projects could not be obtained for publication in the GAO report.) A total of 12 of these 16 credentialing systems are large-scale projects intended to provide identity credentials to an entire agency’s employees, while the remaining four projects are smaller in scale.

Smart card initiatives in government vary widely in size and scale. For instance, the DoD Common Access Card (CAC) has already been deployed to over 4 million personnel and is one of the Federal Government’s best-known credentialing implementations. The CAC includes a digital signature, encryption modules for secure messages, and a hardware token for storage of cryptographic keys to protect unclassified networks and smart card technology. The hardware token serves as an identification card and an enabler for logical and physical access.

On a smaller scale, the Department of Commerce’s National Oceanic and Atmospheric Administration (NOAA) Geophysical Fluid Dynamics Laboratory Access Card is designed to be used by approximately 600 employees. The objective of NOAA’s credential is to facilitate secure log-on to computer terminals.

Table 16 summarizes the 16 ongoing smart card implementations documented in the GAO report.

Table 16. Ongoing Federal Smart Card Technology Initiatives by Department

Federal Agency	Projects	Status	Size	Cards Issued	Population Served
Commerce	2	Operational	Large	5,313	As needed
		Operational	Small	204	612
Defense	2	Operational	Large	2,750,859	3,457,975
		Operational	Large	46,105	15,000 per year
DHS	1	Pilot	Large	0	6,000,000
Interior	3	Planning	Small	0	2,100
		Operational	Large	0	70,000
		Operational	Large	7,100	90,000
Justice	1	Pilot	Large	31	50,000
Labor	1	Operational	Small	768	3,100
NASA	1	Planning	Large	0	85,000
State	1	Operational	Large	45,000	130,000
Transportation	2	Operational	Small	1,200	1,200
		Planning	Large	0	98,853
Treasury	2	Operational	Large	2,500	7,500
		Operational	Large	30,528	75,000

Federal Identity Management Handbook

Source: GAO's Report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives, *Federal Agencies Continue to Invest in Smart Card Technology*, September 2004.

As previously stated, many agencies' smart card initiatives were absorbed by larger-scale implementations. More agencies are currently seeing the benefits of integrated agency-wide smart card efforts. Aside from preventing identity theft, these integrated smart card initiatives enable one interoperable card to be used at numerous government locations for both physical and logical access. Integrated smart card technologies help increase the level of identity assurance while reducing production costs. Nine government agencies currently have such multiuse application projects underway. These efforts are summarized in Table 17.

Table 17. Integrated Federal Smart Card Implementations by Agency

Agency	Project	Status	Completion	Applications Supported
Defense	Common Access Card (CAS)	Operational	April 2003	Identity credential Physical access Logical access
Homeland Security	Identification and Credentialing Program	Pilot	Unknown	Identity credential Physical access Logical access
General Services Administration	Nationwide Identification	Operational	December 2004	Identity credential Physical access
Interior	E-Authentication	Operational	January 2004	Identity credential Physical access Logical access E-signature
Labor	E-Authentication	Planning	April 2005	Identity credential Physical access Logical access
NASA	One NASA Smart Card Badge	Planning	September 2004	Identity credential Physical access Logical access
State	Global Look ID	Operational	September 2006	Identity credential Physical access Logical access E-mail
Treasury	Electronic Treasury Enterprise Card	Operational	September 2004	Identity credential Physical access Logical access Asset management
Veterans Affairs	Authentication and Authorization Infrastructure Project	Pilot	September 2007	Identity credential Physical access Logical access

Federal Identity Management Handbook

Source: GAO's Report to the Subcommittee on Technology, Information Policy, Intergovernmental Relations, and the Census, Committee on Government Reform, House of Representatives, *Federal Agencies Continue to Invest in Smart Card Technology*, September 2004.

As these data indicate, Federal agencies are relying more and more on smart card technologies for identity credentialing and physical access, and the benefits of implementing smart card technologies are becoming clear. Such benefits range from verifying the identity of agency personnel accessing government buildings and computer terminals to managing assets and storing monetary value. In addition, agencies are consolidating their efforts, with smaller-scale initiatives being absorbed by larger initiatives to integrate the smart card technologies and reduce costs and confusion. As agencies begin to consolidate their efforts, the cost of obtaining the technology necessary to implement a smart card-based identity credentialing program is likely to decrease.

5.4.1 U.S. Department of State

The U.S. Department of State was one of the first Federal agencies to implement a multifunctional smart card for physical and logical access control and PKI applications. Although the applications are completely integrated, two bureaus within the State Department separately manage the physical and logical access control systems.

The State Department relied on two Federal credentialing guidelines for assistance in the design and implementation of its system. *Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems Version 2.2* was used in the design of the physical access control system. The State Department deployed its cards in accordance with the standards in the Government Smart Card Interoperability Specification (GSC-IS), making State's cards compatible with those of other complying agencies.

The State Department's smart cards use the file system card edge. Although cards that are supported by the virtual machine (VM) card edge have captured the majority of the smart card market in recent years, VM cards did not have a proven performance record when the State Department began its implementation. File System cards are fully supported in Federal government applications, and FIPS 201 promotes a credentialing system in which either card edge can be selected by an agency, with the assumption that they will be interoperable.

The programmable readers installed at the State Department are able to communicate with different legacy access control systems. A 3-year migration path has been suggested to replace the current legacy access control system.

Approximately 130,000 users will use the new card to access State Department facilities. To date, the State Department has issued the cards to its U.S.-based employees and is in the process of issuing cards overseas. PKI is currently used for encrypting and signing emails on the department's SBU OpenNet (ON) system, for code-signing, and for secure access to State Department web sites. PKI will also be used to provide digital signatures for the new E-Forms application, which the A bureau will deploy. BLADE (Biometric for Logical Access and Development) will be integrated with PKI to replace username/password for access to ON. Once integration is complete, all State Department users will use PKI to log on to their unclassified Windows accounts. As of July 2004, approximately 20,000 desktops support PKI, with the PKI/BLADE rollout planned to be complete by the end of 2006. Biometrics are currently being integrated to control physical access to sensitive areas.

Federal Identity Management Handbook

In the future, the State Department plans to store other data on the smart card, including emergency medical information, human resources data, and travel orders.

5.4.2 U.S. Department of Interior

The Bureau of Land Management (BLM) within the U.S. Department of Interior has one of the most comprehensive smart card deployments, with approximately 20,000 users. BLM forecasts that all 70,000 Bureau users will be issued card tokens by October 2005.

Before deploying its new credential, BLM engaged in a variety of activities that helped the agency complete the process satisfactorily. First, BLM developed a business case to evaluate key business drivers and discriminators for its identity management program. Key performance criteria included a reduction in fixed labor cost, the establishment of a single point of data entry, and the creation of a single, agency-wide credentialing system entirely manufactured from COTS products. BLM documented its business case in the OMB-300 form and submitted it to the OMB for review. Once the document was approved, BLM was assured that its funding and IT process goals were acceptable.

Additionally, BLM met with agencies that had launched major credentialing programs, such as DoD. By researching other agency programs, BLM was able to identify best practices and lessons that could be applicable to its own identity management program. Finally, BLM completed a substantial amount of integration work with smart cards and their associated applications in advance of issuing a solicitation. To this end, it engaged vendors to establish a demonstration lab in which a small-scale credentialing environment was created. The evaluation of the lab's performance enabled BLM to reduce technology and process risks while observing the products in operation.

The cards that BLM is deploying contain a 64-KB contact chip for logical access applications and a separate 4-KB contactless chip for physical access applications. The evolution from a proximity card to a contactless chip for physical access represents a significant achievement for a Federal agency. This migration strategy provides increased security without decreasing the rate at which users are able to access facilities. Moreover, the larger amount of memory available on the contactless chip enables BLM to program the cards so that they can operate with many different readers across multiple locations.

BLM users access network applications by inserting a smart card into a workstation's reader and entering a PIN. Once they are logged on, employees can access many applications and forms that automatically populate user information stored on the card. BLM's contractors can securely access the same system and distribute forms that are signed with digital certificates. For example, oil and gas contractors have found that BLM's eForms streamline the procurement process, providing them with the current status of their proposals and projects.

BLM's migration to online data processing has also proved beneficial to its form management process: the agency's more than 1,000 forms are easily updated on line, ensuring users that they have the correct source document. The result is increased communication speed and decreased volumes of paper and help-desk calls.

While many of BLM's users appreciate the introduction of smart cards into their work environment, there is a perception that authentication to facilities and networks with the new credential takes more time. Users also tend to blame smart cards when other mechanical devices, such as elevators, card

readers, or network directories, fail. To dispel some of these misperceptions, BLM has released a 22-minute training video that conveys BLM's program vision and shares its goal to be a leader in cyber- and physical security while endorsing IT interoperability across government. The training is also available on CD-ROM and the Internet.

5.4.3 U.S. Department of Homeland Security

Transportation Security Administration Transportation Workers Identification Credential

The Transportation Security Administration (TSA) is mandated by Federal legislation to develop an identification system for individuals requiring access to secure areas of the nation's transportation system, including seaports and airports and rail, pipeline, trucking, and mass transit facilities. To meet this requirement, TSA is issuing the Transportation Worker Identification Credential (TWIC), a uniform credential that is designed to enable access to the transportation system. In the prototype phase of the implementation, TSA is distributing the TWIC to approximately 200,000 workers in East Coast, West Coast, and Florida ports. The production phase will issue the TWIC to as many as 6 million workers.

The TWIC is supported by a technical solution that is scalable, secure, and COTS-based. The components are interoperable and nonproprietary, giving TSA flexibility and choice while ensuring that the solution does not lock the government into a single design.

The integrated system provides a comprehensive solution for enrolling and issuing the TWIC to a widely dispersed population. The architecture enables workers and their employers to initiate the enrollment process using a web-based pre-enrollment tool. The worker's identity is authenticated using biometrics, background checks, and identity-proofing documents. The enrollment web site is secure, protects users' privacy rights, and lowers TSA's administration costs.

Once the background checks are passed, the enrollment information is securely transmitted to a card production facility. The cardholders' personal and biometric information is stored on the smart card. Finally, the card is activated through a one-on-one authentication transaction between a Trusted Agent and the cardholder that includes matching the cardholder's fingerprint to the fingerprint stored on the card. Once the cardholder has an active TWIC, logical and physical access to sites can be granted using a variety of biometric technologies including facial recognition, iris scan, hand geometry, and fingerprint. Additionally, the credential can be used within a facility to facilitate multiple levels of access control.

A large number of metrics are being collected and monitored during the prototype phase. The system also makes use of an end-to-end security infrastructure for establishing a chain of trust for the different processes within the system.

Summary

Federal agencies have many resources at their disposal to aid them in implementation of FIPS 201. One of the most important resources is the experience and lessons learned by other agencies who have implemented smart card technology. Many credentialing managers and experts from various agencies are able and willing to provide their insights into best practices for implementing a credentialing

system. Many of these individuals are members of the FICC and IAB. Membership to these two committee's is open to all Federal agencies and their credentialing managers.

5.5 Conformance Testing

Conformance testing is done to ensure that a product meets the requirements described in a specification. Conformance testing detects any deviations from the specification and must define the criteria for determining conformance.

The specification against which the product is tested generally includes test assertions. Test assertions are statements of functionality or behavior that will be true for conforming products. Generally, if a product satisfies all of the test assertions associated with a specification, then it is said to be in conformance with the specification.

Conformance testing is essential to the implementation of a PIV system. Conformance testing is usually performed on a product or a suite of products and produces a set of results. During testing, the results will be evaluated to determine whether they conform to FIPS 201 and associated Special Publications (SP 800-73 and SP 800-76, which are the technical specifications for ICC and biometric data, respectively). If the results conform, they are then used as the baseline against which to compare other test results. Cards and middleware will be tested to ensure that they conform to the specifications defined in FIPS 201, SP 800-73, and SP 800-76. Vendor products that complete and pass the FIPS 201 conformance test suite are considered to be FIPS 201 compliant.

5.5.1 Why Conformance Testing is Needed

Conformance testing is used to determine whether a particular product (or implementation) performs in a manner that complies with the functional and technical requirements of FIPS 201. Conformance testing cannot be used to judge whether one product is superior to another. Conformance testing enables agencies to implement standards-based products.

Conformance testing also promotes interoperability among products, cost savings, and quality. Potential cost savings are realized by agencies as a result of not having to purchase products that do not conform to FIPS 201 and the associated Special Publications. It is important to note that although conformance testing increases the probability that two conformant products will be interoperable, it does not guarantee interoperability. Agencies are encouraged to complete their own tests to prove interoperability and functionality within their own environments. The policies and business processes that agencies implement also affect interoperability.

5.5.2 How Conformance Testing is Performed

Conformance testing generally involves the following components:

- The conformance requirements
- A test tool
- A test program
- Test procedures

Federal Identity Management Handbook

- A test organization (performs the test, publishes results, certifies conformant products/implementations, adjudicates any issues that arise)
- A test report or compliant product listing or both

Figure 20 illustrates the process for testing cards and middleware for conformance to FIPS 201.

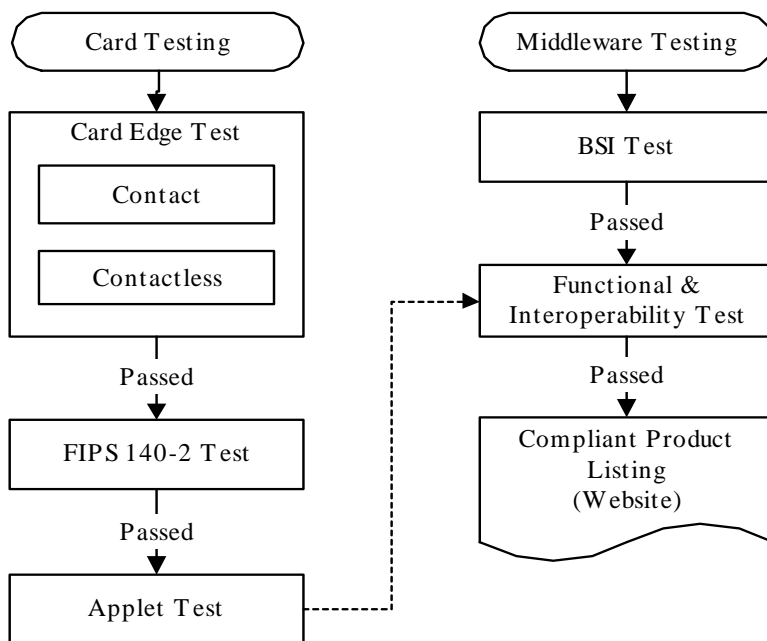


FIGURE 20. FIPS 201 CARD AND MIDDLEWARE TEST PROCESS⁵⁰

The tests for cards and middleware follow separate testing paths that converge at the functional and interoperability test, where integrated conformance testing is performed on end-user applications. The test process is described below.

5.5.2.1 Card Testing

The first step in testing cards is to test the card edge. The card edge communicates directly with the card by using the Application Protocol Data Unit (APDU). FIPS 201 specifies two card edges, contact and contactless. Testing will be conducted on both card edges.

Once the card edge has successfully met all test requirements, the card is submitted for FIPS 140-2 module testing. This testing certifies that the cryptographic modules used on the card meet the requirements in FIPS 140-2. When testing is complete and a certificate of conformance is issued, optional applet testing can begin.

⁵⁰ Figure courtesy of Department of Defense (DoD) Joint Interoperability Test Command (JITC).

Applet testing is agency-specific. Requirements for applets vary from agency to agency. For example, some agencies may want to implement an electronic purse, while others may want to implement an applet that automatically populates on-line forms. Applet testing for functions not required by FIPS 201 and the associated Special Publications is optional, and if it is not desired by an agency, the card can proceed from FIPS 140-2 testing to functional and interoperability testing. If applet testing is required, the PIV card must pass the test defined by the agency before moving to functional and interoperability testing.

5.5.2.2 Middleware Testing

Middleware testing begins with tests on the basic services interface (BSI). The BSI is an application program interface (API) in the middleware. The BSI is the interface between a high level program and APDU commands that the PIV card understands. Testing the BSI tests the ability of the middleware to communicate with a PIV card. Once BSI testing is successful, middleware testing proceeds to functional and interoperability testing.

5.5.2.3 Functional and Interoperability Testing

Functional and interoperability testing tests end-user applications. Utility programs included in the middleware, web browser interfaces, and e-mail signing modules are just some of the applications that could be tested.

5.5.2.4 Post-Test Process

After a product has successfully completed conformance testing, it is added to the compliant product-list web site. The Department of Defense, Defense Information Systems Agency, Joint Interoperability Test Command will host this web site. The web site will eventually list all products that have successfully completed FIPS 201-conformance testing. Agencies can use the web site to research FIPS 201-conformant smart cards and middleware. Agencies can also refer the FICC web site (<http://www.cio.gov/ficc/>) for FIPS 201-compliant products.

5.5.2.5 Testing Organization Requirements

The organization responsible for conformance testing needs to be composed of impartial experts who have no stake in the outcome of the tests. This ensures that testing is done fairly and the results are not influenced in any way.

Additional test tools, test plans, and test procedures will be developed in the coming months to support compliance testing of FIPS 201 products. Agencies should check the NIST web site, <http://csrc.nist.gov/piv-project/index.html>, or the FICC web site for further details.

Summary

Products that successfully pass and complete the FIPS 201 conformance test are considered FIPS 201 compliant. The results of conformance testing provide agencies with a valuable resource. The publication of test results and the compliant product registry provide agencies with a list of conforming and nonconforming products. Agencies are also encouraged to conduct pilots and delay full-scale

implementation until they have evaluated how the components they want to implement for FIPS 201 will behave in their environment.

5.6 Reference Implementation

To assist Federal agencies in their technical understanding of a PIV system implementation, the Government commissioned development of a PIV Reference Implementation. The objective of the Reference Implementation is to produce a software framework within which to test candidate PIV cards and client applications that use the PIV card. The functionality of the PIV Reference Implementation is defined by SP 800-73, *Integrated Circuit Card for Personal Identity Verification*.⁵¹ SP 800-73 is the technical companion to FIPS 201 and provides all the technical details needed to build interoperable PIV cards and PIV client-application programming interface middleware.

The PIV Reference Implementation complies with the technical specifications of SP 800-73 and provides an environment in which the interoperation of client application programs, the PIV card application, and other card applications can be assessed. Figure 21 is a diagram of the PIV Reference Implementation architecture. In addition to the PIV card application, other card applications can be loaded into either the Java Card runtime environment or into the native code runtime environment and run with the PIV card application.

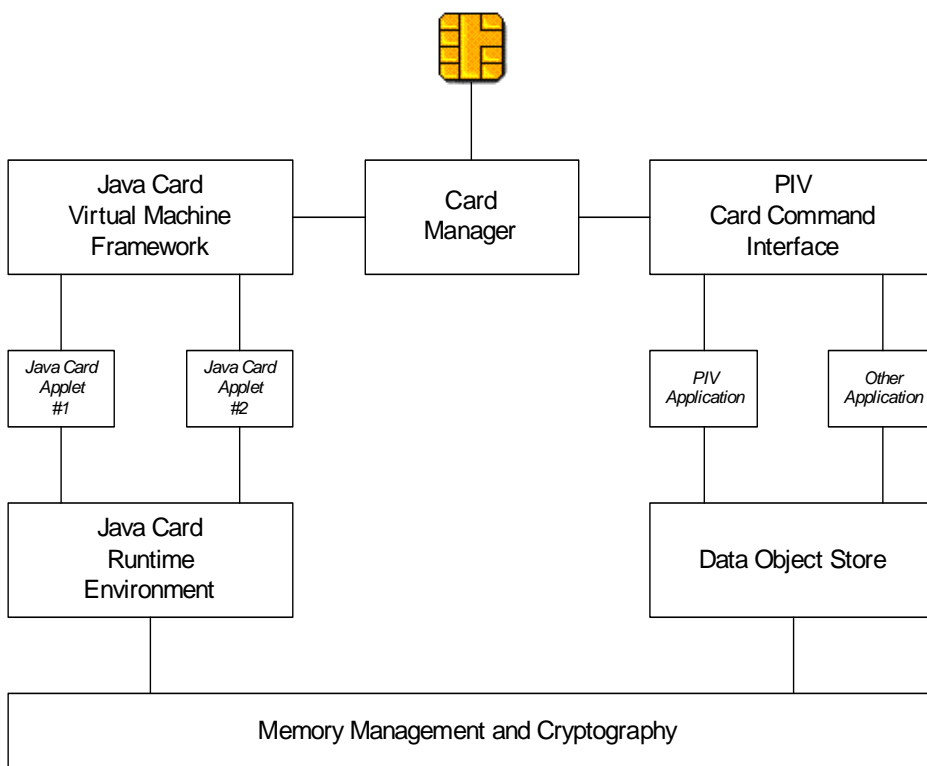


FIGURE 21. NIST REFERENCE IMPLEMENTATION ARCHITECTURE⁵²

The PIV Reference Implementation is being created by NIST and is expected to be completed in the summer of 2005. It will be made available to agencies on CD-ROM and through the Internet. The

⁵¹ Special Publication 800-73, *Integrated Circuit Card for Personal Identity Verification*, NIST, February 2005.

⁵² NIST Reference Implementation.

Federal Identity Management Handbook

final product will include source code and an executable program that will enable PIV card simulation. Detailed instructions describing how to install, build, and execute the PIV Reference Implementation will be included.

Agencies can also use the PIV Reference Implementation as part of the PIV system component acquisition process. Because the PIV Reference Implementation meets the requirements of SP 800-73, agency solicitations may require that vendor products perform satisfactorily with the PIV Reference Implementation. By requiring compliance with the Reference Implementation, agencies may be able to avoid conducting user acceptance tests to ensure interoperability of the PIV system components they procure.

Regardless of who conducts the testing (an agency or a vendor), the test will only apply to cards that comply with the SP 800-73 specifications. However, agencies can use the PIV Reference Implementation to test their own agency-specific card applications in addition to the PIV card application. To do this, the agency-specific card applications are loaded into the PIV Reference Implementation and tested in coordination with the PIV card application.

6. APPENDIX A – Sample Acquisition Planning Template

Acquisition Plan Title:

Prepared by:

Name _____

Title _____

Office _____

Telephone Number _____

Date _____

Approvals:

Name _____

Title _____

Office _____

Telephone Number _____

Date _____

Acquisition Planning Template

<p>1.0</p>	<p><u>Statement of Need</u> <i>Introduce the plan with a brief statement of need. Summarize the technical and contractual history of the acquisition. Discuss feasible acquisition alternatives, the impact of prior acquisitions on those alternatives, and any related in-house effort.</i></p> <p><i>These acquisition requirements are in response to HSPD-12 and the subsequent FIPS 201 specifications developed by NIST.</i></p>
<p>1.1</p>	<p><u>Background</u> HSPD-12 was issued on August 27, 2004. It establishes a policy for a common identification standard for Federal employees and contractors. The Secretary of Commerce, with direct involvement of NIST, was tasked with developing the standard. The acquisition plan described herein is designed to meet the requirements of HSPD-12/FIPS 201.</p>
<p>1.2</p>	<p><u>Acquisition Alternatives</u> <i>List different methods to obtain services:</i></p> <ul style="list-style-type: none"> - <i>GSA Smart Access Common ID Contract</i> - <i>Individual GSA schedules</i> - <i>Aggregated Buy</i>
<p>2.0</p>	<p><u>Applicable Conditions</u> <i>State all significant conditions affecting the acquisition, such as</i></p> <ul style="list-style-type: none"> <i>(i) Requirements for compatibility with existing or future systems or programs</i> <i>(ii) Known cost, schedule, and capability or performance constraints.</i>
<p>3.0</p>	<p><u>Cost</u> <i>Set forth the established cost goals for the acquisition and the rationale supporting them and discuss related costs including, as appropriate, costs included in Section 3.1 below.</i></p> <p><i>Discussion of the thought process that goes into cost development.</i></p>
<p>3.1</p>	<p><u>Life-Cycle Cost of FIPS 201 Implementation</u> <i>Include other costs as appropriate:</i></p> <ul style="list-style-type: none"> - <i>Maintenance costs</i> - <i>Replacement costs</i> - <i>Upgrade costs (i.e., technology improvements)</i> - <i>Integration costs (i.e., project management costs)</i>

Federal Identity Management Handbook

4.0	<p><u>Capability or Performance</u></p> <p>Specify the required capabilities or performance characteristics of the supplies or the performance standards of the services being acquired and state how they are related to the need.</p> <p><i>High-level discussion:</i></p> <ul style="list-style-type: none"> - All items being procured satisfy the requirements of FIPS 201, which are (for example) 64K contact/contactless card, biometric fingerprint capture device. - These additional items, although not required by FIPS 201, are necessary for agency specific requirements: (for example) PKI – for logical access to systems/networks/applications
5.0	<p><u>Delivery or Performance-Period Requirements</u></p> <p>Describe the basis for establishing delivery or performance-period requirements. Explain and provide reasons for urgency if development and production must proceed concurrently or if urgency constitutes justification for not providing for full and open competition.</p>
6.0	<p><u>Trade-Offs</u></p> <p>Discuss the expected consequences of trade-offs among the various cost, capability or performance, and schedule goals.</p>
7.0	<p><u>Risks as identified in OMB Agency Plan</u></p> <p>Discuss technical, cost, and schedule risks and describe what efforts are planned or underway to reduce risk and the consequences of failure to achieve goals. If development and production will proceed concurrently, discuss the effects on cost and schedule risks.</p>
8.0	<p><u>Acquisition Streamlining</u></p> <p>If specifically designated by the requiring agency as a program subject to acquisition streamlining, discuss plans and procedures to</p> <ul style="list-style-type: none"> (i) Encourage industry participation by using draft solicitations, pre-solicitation conferences, and other means of stimulating industry involvement during design and development in recommending the most appropriate application and tailoring of contract requirements. (ii) Select only the necessary and cost-effective requirements. (iii) State the timeframe for identifying which of the specifications and standards originally provided as guidance only, shall become mandatory. <p><i>Participate in Government-wide acquisition methods such as:</i></p> <ul style="list-style-type: none"> - SSP - Aggregated buy - GSA Smart Access Common ID Contract

	<p><i>Plan of Action</i></p>
1.0	<p><u>Sources</u></p> <p>Indicate prospective sources of supplies or services that can meet the need. Consider required sources (see Part 8). Include consideration of small business, veteran-owned small business, service-disabled veteran-owned small business, HUBZone small business,</p>

Federal Identity Management Handbook

	<i>Plan of Action</i>
	<i>small disadvantaged business, and women-owned small business concerns (see Part 19), and the impact of any bundling that might affect their participation in the acquisition (see Part 7.107) (15 U.S.C. 644(e)). Address the extent and results of the market research and indicate the impact of such research on the various elements of the plan (see Part 10).</i>
2.0	<p><u>Competition</u></p> <p><i>Describe how competition will be sought, promoted, and sustained throughout the acquisition process. If full and open competition is not contemplated, cite the authority in 6.302, discuss the basis for the application of that authority, identify the sources, and discuss why full and open competition is not possible.</i></p>
2.1	<p><u>Competition, Component Breakout</u></p> <p><i>Identify the major system components or subsystems. Discuss component breakout plans relative to these major components or subsystems. Describe how competition will be sought, promoted, and sustained for acquisition of these components or subsystems.</i></p> <p><i>Example: The major components are:</i></p> <ul style="list-style-type: none"> ○ <i>Biometric capture devices: fingerprint and facial</i> ○ <i>IDMS: Systems or applications that manage the identity verification, validation and issuance process</i> ○ <i>Enrollment equipment: Computer monitor/key board, PIN pad, camera, network connection, back-end database, software</i> ○ <i>Card issuance system: Cards, printers/consumables</i> ○ <i>Card management system: Monitor, keyboard, database, network connectivity, software</i> ○ <i>Physical access control system: Readers, turnstiles, PIN pads, back-end system, software</i> ○ <i>Logical access control: Readers, middleware, PKI (necessary systems/components), software</i> ○ <i>Central management / Integration services</i>
2.2	<p><u>Competition, Spares, and Repair Parts</u></p> <p><i>Describe how competition will be sought, promoted, and sustained for acquisition of spares and repair parts. Identify the key logistic milestones, such as technical data delivery schedules and acquisition method coding conferences that affect competition.</i></p>
2.3	<p><u>Competition, Subcontracts</u></p> <p><i>When effective subcontract competition is both feasible and desirable, describe how such subcontract competition will be sought, promoted, and sustained. Identify any known barriers to increasing subcontract competition and address how to overcome them.</i></p>
3.0	<p><u>Source Selection Procedures</u></p> <p><i>Discuss the source-selection procedures for the acquisition, including the timing for submission and evaluation of proposals and the relationship of evaluation factors to the attainment of the acquisition objectives.</i></p>
4.0	<p><u>Contracting Considerations</u></p> <p><i>For each contract contemplated, describe the use of multiyear contracting, options, or other special contracting methods (see Part 17); any special clauses, special solicitation provisions, or FAR deviations required (see Subpart 1.4); whether sealed bidding or</i></p>

Federal Identity Management Handbook

	<i>Plan of Action</i>
	<i>negotiation will be used and why; whether equipment will be acquired by lease or purchase (see Subpart 7.4) and why; and any other contracting considerations.</i>
4.1	<p><u>Contract Type</u></p> <p><i>For each contract contemplated, discuss contract type selection (see Part 16) and use of multiyear contracting, options, or other special contracting methods (see Part 17);</i></p>
4.2	<p><u>Lease or Purchase</u></p> <p><i>Contemplate whether equipment will be acquired by lease or purchase (see FAR Subpart 7.4)</i></p>
4.3	<p><u>Performance-Based</u></p> <p><i>If a performance-based contract will not be used or if a performance-based contract for services is contemplated on other than a firm-fixed price basis, provide a rationale for these decisions (see 37.102(a) and 16.505(a)(3)). Acquisition plans for service contracts must describe the strategies for implementing performance-based contracting methods or must provide a rationale for not using those methods.</i></p>
5.0	<p><u>Budgeting and Funding</u></p> <p><i>Include budget estimates, explain how they were derived, and discuss the schedule for obtaining adequate funds at the time they are required (see FAR 32.7).</i></p>
6.0	<p><u>Product or Service Descriptions</u></p> <p><i>Explain the choice of product or service description types (including performance-based contracting descriptions) to be used in the acquisition.</i></p>
7.0	<p><u>Priorities, Allocations, Allotments</u></p> <p><i>When urgency dictates a particularly short delivery or performance schedule, certain priorities may apply. If so, specify the method for obtaining and using priorities, allocations, and allotments, and the reasons for them (see Subpart 11.6).</i></p>
8.0	<p><u>Contract versus Government Performance</u></p> <p><i>Address the consideration given to OMB Circular No. A-76 (see Subpart 7.3).</i></p>
9.0	<p><u>Inherently Governmental Functions</u></p> <p><i>Address the consideration given to OFPP Policy Letter 92-1 (see Subpart 7.5).</i></p> <p><i>The following roles, identified in FIPS 201, must be the responsibility of an authorized government employee:</i></p> <ul style="list-style-type: none"> - <i>PIV Sponsor</i> - <i>PIV Registrar</i> - <i>PIV Issuer</i>
10.0	<p><u>Management Information Requirement</u></p> <p><i>Discuss, as appropriate, what management system will be used by the government to monitor the contractor's effort.</i></p>
11.0	<p><u>Make or Buy</u></p> <p><i>Discuss any consideration given to make-or-buy programs.</i></p> <p><i>Include a GOTS vs. COTS discussion, assuming that as a result of the issuance of FIPS 201, many companies will develop FIPS 201-compliant GOTS products.</i></p>
12.0	<u>Test and Evaluation:</u>

Federal Identity Management Handbook

	<i>Plan of Action</i>
	<i>Discuss the conformance testing that has been done on FIPS 201 products.</i>
13.0	<u>Logistics Consideration</u> <i>Describe 13.1, 13.2, 13.3 and 13.4, below</i>
13.1	<u>Assumptions Concerning Contractor or Agency Support</u> <i>Describe the assumptions determining contractor or agency support, both initially and over the life of the acquisition, including consideration of contractor or agency maintenance and servicing (see Subpart 7.3) and distribution of commercial items</i>
13.2	<u>Quality Assurance, Reliability, Maintainability, Warranties</u> <i>Describe reliability, maintainability, and quality assurance requirements, including any planned use of warranties (see Part 46);</i>
13.3	<u>Requirements For Contractor Data</u> <i>Describe the requirements for contractor data (including repurchase data) and data rights, their estimated cost, and the use to be made of the data (see Part 27);</i>
13.4	<u>Standardization Concepts</u> <i>Discuss any standardization concepts, including the necessity to designate (in accordance with agency procedures) technical equipment as "standard" so that future purchases of the equipment can be made from the same manufacturing source.</i>
14.0	<u>Government Furnished Property</u> <i>Indicate any property to be furnished to contractors, including materials and facilities, and discuss any associated considerations, such as the availability of such property or a schedule for its acquisition (see Part 45).</i>
15.0	<u>Milestones For The Acquisition Cycle</u> <i>Address the following steps and any others considered appropriate:</i> <ul style="list-style-type: none"> • <i>Acquisition plan approval</i> • <i>Statement of work</i> • <i>Specifications</i> • <i>Data requirements</i> • <i>Completion of acquisition-package preparation</i> • <i>Purchase request</i> • <i>Justification and approval for other than full and open competition where applicable and/or any required D&F approval</i> • <i>Issuance of solicitation</i> • <i>Evaluation of proposals, audits, and field reports</i> • <i>Beginning and completion of negotiations</i> • <i>Contract preparation, review, and clearance</i> • <i>Contract award</i>
16.0	<u>Identification Of Participants In Acquisition Plan Preparation</u> <i>List the individuals who participated in preparing the acquisition plan, giving contact information for each.</i>

7. APPENDIX B – Implementation Checklist

ID#	Task	Applicable FIPS 201 Section	Status (Not Started, In-progress, Complete)	Completion or Scheduled Completion Date	Responsible Organization	Responsible Individual/phone #
PIV I – Compliance by October 25, 2005						
Identity Proofing		2.2				
1	Identity proofing and registration process is accredited by department or agency Inspector General					
2	Identity proofing and registration process is approved in writing by the head of department or agency					
3	A NACI has been initiated or a completed NACI is on record for all employees and contractors					
4	A NAC has been completed and adjudicated for all employees and contractors prior to credential issuance					
5	All credential applicants have appeared in-person at least once to an individual responsible for credential issuance in your department or agency					
6	All applicants have provided 2 forms of original documentation included in the Form I-9, OMB No. 1115-0136, Employment Eligibility Verification					
7	At least one of the documents listed in ID # 6 above is a valid State or Federal Government issued picture ID					
8	Agency's identity proofing, registration, and issuance processes does not allow one individual to issue a credential without the cooperation of at least one other approved individual					
Issuance and Maintenance		2.3				
9	Issuance and maintenance process is accredited by department or agency Inspector General					
10	Issuance and maintenance process is approved in writing by the head of department or agency					

Federal Identity Management Handbook

11	Issuance and maintenance process ensures the completion and successful adjudication of a NAC, NACI, or another OPM or National Security community investigation as required for Federal employment. (If the results of the investigation so dictate the credential shall be revoked)					
12	Prior to the release of a PIV credential to an applicant, the issuer must complete the chain of trust by verifying that the photograph in the registration or enrollment record matches the applicant. Upon successful match, the issuer shall release the PIV credential to the applicant					
13	The NAC must be completed and adjudicated before issuance can take place					
14	Agencies must issue credentials through systems and providers whose reliability has been established by the agency and so documented and approved in writing					
Privacy		2.4				
15	Assign an individual to the role of senior agency official for privacy					
16	Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with the E-government act of 2002 and OMB Memorandum M-03-22, as applicable					
17	Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected, 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 of agency					
18	Assure that systems that contain information in identifiable form for the					

Federal Identity Management Handbook

	purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in the Privacy Act of 1974					
19	Maintain appeals procedures for those who are denied a credential or whose credentials are revoked					
20	Ensure that only personnel with a legitimate need for access to information in identifiable form in the PIV system are authorized to access IIF, including but not limited to information and databases maintained for registration and credential issuance					
21	Coordinate with the appropriate department or agency officials to define consequences for violating privacy policies of the PIV system					
22	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					
23	Utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable					
24	Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of IIF					

Federal Identity Management Handbook

ID#	Task	Applicable FIPS 201 Section	Status (Not Started, In-progress, Complete)	Scheduled Completion	Responsible Organization	Responsible Individual/phone #
PIV II – Compliance provided by OMB Implementation Guidance						
<u>Physical PIV Card Topology</u>		4.1				
25	The PIV Card shall comply with physical characteristics as described in: <ul style="list-style-type: none"> • ISO 7810 • ISO 10373 • ISO 7816 • ISO 14443 					
<u>Printed Material</u>		4.1.1				
26	The printed material shall not rub off during the life of the PIV Card					
27	The printing process shall not deposit debris on the printer rollers during printing and laminating					
<u>Tamper Proofing and Resistance</u>		4.1.2				
28	Printed material shall not interfere with the contact and contactless ICC(s) and related components, nor shall it obstruct access to machine-readable information					
29A	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: Optical varying structures, Optical varying inks, Laser etching and engraving, Holograms, Holographic images, Watermarks)					
29B	Incorporation of security features shall: <ul style="list-style-type: none"> • Be in accordance with durability requirements [ISO7810] • Be free of defects, such as fading and discoloration • Not obscure printed 					

Federal Identity Management Handbook

	<p>information</p> <ul style="list-style-type: none"> • Not impede access to machine-readable information 					
<u>Physical Characteristics and Durability</u>		4.1.3				
30	The PIV Card shall contain a contact and a contactless ICC interface					
31	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					
32	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					
32	The card shall be 27- to 33-mil thick (before lamination) in accordance with ISO7810					
33	The PIV Card shall not be embossed					
34	Decals shall not be adhered to the card					
35	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					

Federal Identity Management Handbook

	material shall allow production of a flat card in accordance with ISO7810 after lamination of one or both sides of the card.					
<u>Mandatory Items on the Front of the PIV Card</u>		4.1.4.1				
36	Zone 1—Photograph. The photograph shall be placed in the upper left corner and be a full frontal pose from top of the head to shoulder, as depicted in Figure 4-1. A minimum of 300 dots per inch (dpi) resolution shall be used. The background should follow recommendations set forth in SP 800-76					
37	Zone 2—Name. The full name shall be printed directly under the photograph in capital letters. The font shall be a minimum of 10 point					
38	Zone 8—Employee Affiliation. A printed employee affiliation shall be printed on the card. Some examples of employee affiliation are “CONTRACTOR,” “ACTIVE DUTY,” and “CIVILIAN.”					
39	Zone 10— Organizational Affiliation					
40	Zone 14—Expiration Date. The card expiration date shall be printed in a YYYYMMDD format					
<u>Mandatory Items on the Back of the Card</u>		4.1.4.2				
41	Zone 1—Agency Card Serial Number. Must contain the unique serial number from the issuing department or agency. The format shall be at the discretion of the issuing department or agency					
42	Zone 2—Issuer Identification. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or					

Federal Identity Management Handbook

	agency					
Logical Credential Data Model		4.1.5.1				
43	Mandatory data elements: <ul style="list-style-type: none"> • PIN • CHUID • PIV authentication data (one asymmetric key pair and corresponding certificate) • Two biometric fingerprints 					
PIV Card Activation		4.1.6				
44	The PIV Card must be activated to perform privileged operations such as reading biometric information and using asymmetric keys					
Activation by Cardholder		4.1.6.1				
45	PIV Cards shall implement PIN-based cardholder activation to allow privileged operations using PIV credentials held by the card					
Activation by Card Management System		4.1.6.2				
46	To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with SP800-73					
47	When cards are personalized, card management keys shall be set to be specific to each PIV Card					
48	Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Recommendation for Cryptographic Algorithms and Key Sizes					
Cardholder Unique Identifier (CHUID)		4.2				
49	The PIV Card shall include the CHUID as defined in SP800-73					
PIV CHUID Data Elements		4.2.1				
50	The CHUID shall include an expiration date. In machine-readable format, the expiration date data element shall specify when the card expires. The expiration date					

Federal Identity Management Handbook

	format and encoding rules are as specified in SP800-73					
<u>Asymmetric Signature Field in CHUID</u>		4.2.2				
51	This standard requires inclusion of the Asymmetric Signature field in the CHUID container					
<u>Logical Access</u>		4.3				
52	At least one asymmetric key must be stored as the PIV key					
53	Cryptographic operations with the mandatory key must be performed through the contact interface					
54	All cryptographic operations, whether using the mandatory or optional keys, shall be performed on-card					
55	All cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above					
56	The PIV card shall provide Level 3 physical security to protect the PIV private keys in storage					
57	The PIV card shall not export the PIV authentication key					
58	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					
<u>Biometric Data Specifications</u>		4.4				
59	A full set of fingerprints for a background check, electronic facial image, and two electronic fingerprints are collected during the identity proofing					
60	The two fingerprints shall be accessible only over the contact interface and after presentation of a valid PIN					
<u>Biometric Data Representation and Protection</u>		4.4.2				
61	PIV biometric data records shall be embedded in a data structure conforming to the Common Biometric					

Federal Identity Management Handbook

	Exchange Formats Framework					
62	PIV biometric data will not be readable in the clear and is protected by an authentication mechanism					
63	An electromagnetically opaque sleeve or other technology is required to protect the biometric data					
Contact Reader Specifications		4.5.1				
64	Contact readers shall conform to ISO 7816 standard for the card-to-reader interface and the PC/SC specification for the reader-to-host system interface					
Contactless Reader Specifications		4.5.2				
65	Contactless readers shall conform to ISO 14443 standard for the card-to-reader interface and the PC/SC specification for the reader-to-host system interface					
<u>PIN Input Device Specifications</u>		4.5.3				
66	PIN input devices shall be used for implementing PIN-based PIV card activation					
<u>PIV II Identity Proofing and Registration Requirements</u>		5.2				
67	All PIV-II identity proofing and registration systems must satisfy the PIV-I objectives and requirements stated in Section 2.2 in order to be approved					
68	An additional requirement for PIV-II is that the biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during the identity proofing and registration process					
<u>PIV Card Issuance</u>		5.3.1				
69	All PIV-II issuance and maintenance systems must satisfy the PIV-I objectives and requirements stated in Sections 2.3 in order to be approved					
70	The process must verify successful completion and adjudication of the NACI within six months of PIV card issuance, or the PIV					

Federal Identity Management Handbook

	card and the PIV authentication certificate for the card shall be revoked					
71	The issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record					
PIV Card Maintenance		5.3.2				
72	The PIV system must ensure that information concerning PIV card renewal, reissuance, PIN reset, and termination is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder					
PIV Card Renewal		5.3.2.1				
73	The card issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials					
74	When renewing identity credentials to current employees, the NACI checks shall be followed in accordance with the OPM guidance					
75	The PIV Card shall be valid for no more than five years					
76	A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card					
77	The card issuer will verify the cardholder's identity against the biometric information stored on the expiring card					
78	The expired PIV Card must be collected and destroyed					
79	The same biometric data may be reused with the new PIV Card while the digital signature must be recomputed with the new FASC-N					
80	The expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card					
PIV Card Reissuance		5.3.2.2				

Federal Identity Management Handbook

81	The entire registration and issuance process, including fingerprint and facial image capture, shall be conducted					
82	The card issuer shall verify that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials					
83	<p>Normal operational procedures must be in place to ensure the following:</p> <ul style="list-style-type: none"> • The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status • The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked • Online Certificate Status Protocol (OCSP) responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately 					
PIV Card PIN Reset		5.3.2.3				
84	Before the reset PIV Card is provided back to the cardholder, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card					
PIV Card Termination		5.3.2.4				
85	<p>The PIV Card shall be terminated under the following circumstances:</p> <ul style="list-style-type: none"> • An employee separates (voluntarily or involuntarily) from Federal service • An employee separates (voluntarily or involuntarily) from a Federal contractor • A contractor changes positions and no longer needs access to Federal buildings or systems • A cardholder is determined to hold a 					

Federal Identity Management Handbook

	<p>fraudulent identity</p> <ul style="list-style-type: none"> • A cardholder passes away 					
86	<p>Normal termination procedures must be in place as to ensure the following:</p> <ul style="list-style-type: none"> • The PIV Card is collected and destroyed • The PIV Card itself is revoked • The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked • OCSP responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately • The IIF that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency 					
PIV Key Management						
87	<p>The certificate authority that issues X.509 certificates shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI. Self-signed, self-issued, and CA certificates shall conform to Worksheets 1, 2, and 3 in <i>X.509 Certificate and CRL Profile for the Common Policy</i></p>	5.4.1				
88	<p>All certificates shall be issued under the id-CommonHW policy and id-CommonAuth policy as defined in the <i>X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework</i></p>	5.4.2				
89	<p>CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to Worksheet 4 of <i>X.509 Certificate and CRL Profile for the Common Policy</i></p>	5.4.3				
90	<p>CA certificates and CRLs will be distributed using</p>	5.4.5.1				

Federal Identity Management Handbook

	LDAP and HTTP					
91	Online Certificate Status Protocol responders shall be implemented as a supplementary certificate status mechanism	5.4.5.2				
<u>Identity Authentication Assurance Levels</u>		6.1				
92	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: <ul style="list-style-type: none"> • 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 					
<u>PIV Validation, Certification, and Accreditation</u>						
93	PIV Card Issuers are certified by appropriate agency authority	App. B1				
94	PIV IT Systems are certified by appropriate agency authority					
<u>OMB Implementation Guidance</u>						
95	Prepare and submit an HSPD-12 agency plan by June 27, 2005					
96	Submit a report to OMB that recommends additional facilities, information systems or other applications that should be included under FIPS 201.					
97	Implement the requirements for FIPS 201 PIV I by October 27, 2005					
98	Implement the requirements for FIPS 201 PIV II by October 27, 2006					

Federal Identity Management Handbook

99	Update the agency's System of Record as needed.					
100	Meet the requirements of OMB-05-05 and comply with the PKI Common Policy Framework by either cross-certifying with the Federal Bridge or procure PKI services from an approved Shared Service Provider.					

8. APPENDIX C – Sample PIV Request Form

<u>Sample PIV Request Form</u>		
Section I: Applicant Information		
First Name:	Last Name:	DOB:
Position / Job Title:	Organization Currently Assigned to:	
Home Address:	Home Phone Number:	Home E-mail:
Work Address:	Work Phone Number:	Work E-mail:
Section II: PIV Sponsor Information. <u>Sponsor must sign in Section V</u>		
First Name:	Last Name:	
Position / Job Title	Organization:	
Work Address:	Work Phone Number:	Work E-mail:
Section III: PIV Registrar.		
First Name:	Last Name:	
Position / Job Title	Organization:	
Work Address:	Work Phone Number:	Work E-mail:
Section IV: PIV Issuer		
First Name:	Last Name:	
Position / Job Title	Organization:	
Work Address:	Work Phone Number:	Work E-mail:
Section V: Signature of PIV Sponsor		
Sign Here:		

9. APPENDIX D – GSA Technical Supplement to OMB M-05-05



March 3, 2005

Dear CIO Member:

On December 20, 2004, the Office of Management and Budget (OMB) issued memorandum M-05-05 “Electronic Signatures: How to Mitigate the Risk of Commercial Managed Services.” This technical supplement provides additional information on the Shared Service Provider Program prescribed for agency use in the OMB memorandum.

Definitions and Scope

“Electronic signature” used in M-05-05 refers to technology used for identity assurance in addition to the act of affixing a legal signature to a document.

The scope of these memos is limited to Public Key Infrastructure (PKI), a cryptographically based “signature” solution. Specifically, these memos cover the deployment of PKI digital certificates to Federal employees and contractor staff on behalf of their employing agencies. They do not refer to Government-to-business or Government-to-citizen relationships. The activities of the E-Authentication initiative address credentialing and electronic signatures in these relationships.

Technical Requirements

To meet the requirements of M-05-05, agencies must be compliant with the Federal PKI Common Policy Framework, the standard policy for the deployment and use of digital certificates for Federal employees, contractors and affiliates.⁵³

All agency implementations of PKI must comply with the Common Policy Framework by October 25, 2005. This can be achieved in one of two ways:

⁵³X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, available at <http://www.cio.gov/ficc/documents/CommonPolicy.pdf>, November 1, 2004.

1. **Cross-Certification with the Federal Bridge** — Agencies operating a Certification Authority that is cross-certified with the Federal Bridge at medium assurance or higher are operating in accordance with the Common Policy. Agencies operating a Certification Authority that is not cross-certified with the Federal Bridge at medium assurance or higher must achieve cross-certification by December 31, 2005, or migrate to compliance with the Common Policy Framework via a Shared Service Provider. Subsequently, the Federal PKI Policy Authority will no longer accept applications for cross certification from Federal organizations unless such requests are accompanied by specific approval from OMB. All future cross certification activities will be reserved for facilitating interoperability with external entities (e.g. states, industry, academia, allied governments).
2. **Shared Service Provider Program** — Agencies that do not meet the criteria above are required to purchase PKI services from entities on the Shared Service Provider list posted at www.cio.gov/ficc, when implementing PKI for their employees and contract staff. Entities included on the Shared Service Provider list have undergone a review process in order to ensure their compliance with the Federal PKI Common Policy Framework and are specifically authorized to issue certificates under the Common Policy.

Access Certificates for Electronic Services

The Access Certificates for Electronic Services (ACES) program administered by General Services Administration (GSA) provides PKI services to a large variety of communities, including unaffiliated individuals, business affiliates, and Federal employees. The majority of ACES services are unaffected by this requirement and continue to be a viable solution for Government-to-citizen, Government-to-business, and Government to Government interactions. Only the Federal Employee PKI Certificate service within ACES is required to undergo review to join the Shared Service Provider program. This is underway. The ACES Federal Employee PKI Certificate services will complete the process and be recognized as Shared Service Providers by October 25, 2005.

Impact of Homeland Security Presidential Directive (HSPD) 12

HSPD-12 requires the use of identification credentials by Federal employees and contractors that meets a government-wide standard. This standard includes access to federally controlled information systems. To meet the logical access requirements of HSPD-12, the standard will specify that agencies must be compliant with the Federal PKI Common Policy Framework discussed above. This ensures agencies compliance with both M-05-05 and HSPD-12 and promotes interoperability across the Government.

Federal Identity Management Handbook

- 3 -

For questions regarding this memorandum, contact Judith Spencer, Office of Governmentwide Policy, General Services Administration, phone (202) 208-6576, fax (202) 501-6455, e-mail: judith.spencer@gsa.gov.

Sincerely,

G. Martin Wagner
Associate Administrator

10. INDEX

Placeholder