



## **Basic Elements that Enable Inter-organizational Trust of Personal Identity Verification (PIV) Cards**

Version 1.0.0  
October 31, 2007



## Document History

Status	Release	Date	Comment	Audience
Draft	0.0.0	7/16/07	Initial draft	Internal
Draft	0.0.1	7/27/07	Revised per Chris Loudon comments	Internal
Draft	0.0.2	7/30/07	Revised per internal review	Judy Spencer
Draft	0.0.3	7/30/07	Revised per Judy Spencer	FICC Working Group
Draft	0.0.4	8/17/07	Revised per FICC Working Group comments	FICC Working Group
Draft	0.1.0	9/07/07	Revised per FICC Working Group final comments	FICC
Final	1.0.0	10/31/07	Released for general distribution	

## Editors

Dave Silver	Chris Loudon	Steve Lazerowich
Judy Spencer	FICC Governance Working Group	

## Executive Summary

Personal Identity Verification (PIV) standards and guidelines include protective measures that establish a reasoned basis for trust of PIV Cards within the federal government. To advocate and outline the case for inter-organization trust of PIV Cards, this document identifies the basic elements that exist as a prerequisite to trust. The elements of trust are discussed in terms of:

- Well-defined standards;
- Compliance regimen that ensures parties adhere to the well-defined standards;
- Relying Party verification whereby relying parties can verify compliance when trusting; and
- Secure components inherent to the PIV Card

Inter-organizational trust of PIV Cards is crucial to HSPD-12 because of the following benefits provided to various communities of interest:

- The federal government benefits by :
  - Reduction of proprietary, duplicative methodology
  - Seamless government-wide interoperability
  - Single government-wide technical standard
  - Government-wide cost savings and efficiencies
  - Contribution to the Homeland Security mission as PIV Cards inherently “enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy”<sup>1</sup>
- Individual agencies benefit in that:
  - Fewer card types for guards and equipment to process, lowering training time and costs
  - Easier and faster visitor processing
  - Fewer card types increases ability to become more expert, as well as detect and discern problems and breaches
  - Standard card across an agency’s sub-organizations
  - Potential for improved access control at both the physical and logical perimeter
- End-Users benefit by:
  - Single card access to all federal locations
  - Simplified identity verification
  - Physical and logical access on a single card
  - Resistance to identity theft

The value of inter-organizational trust of PIV Cards is significant and compelling – to the federal government as a whole and to individual agencies; it encompasses security enhancement and flexibility, cost savings, expedited processing, and enhanced convenience. In the future, the trust element has the potential to seamlessly leverage future PIV innovations and enhancements.

---

<sup>1</sup> [HSPD-12]

## Table of Contents

<b>1. INTRODUCTION .....</b>	<b>5</b>
1.1 BACKGROUND.....	5
1.2 SCOPE .....	5
1.3 APPROACH.....	5
1.4 BENEFITS OF INTER-ORGANIZATION TRUST .....	5
1.4.1 <i>Federal Government</i> .....	5
1.4.2 <i>Individual Agency</i> .....	6
1.4.3 <i>End Users</i> .....	6
<b>2. ELEMENTS OF TRUST .....</b>	<b>7</b>
2.1 WELL-DEFINED STANDARDS .....	7
2.2 COMPLIANCE REGIMEN.....	7
2.3 RELYING PARTY VERIFICATION .....	8
2.3.1 <i>Verify Physical PIV Card Integrity</i> .....	8
2.3.2 <i>Verify Biometrics</i> .....	8
2.3.3 <i>Verify Electronic Signatures</i> .....	8
2.3.4 <i>Certificate Path Discovery</i> .....	9
2.3.5 <i>Certificate Validation</i> .....	9
2.3.6 <i>Rapid Electronic Authentication</i> .....	9
2.4 SECURE COMPONENTS .....	9
<b>3. CONCLUSION .....</b>	<b>10</b>
<b>APPENDIX A: PIV CARD SECURITY HIGHLIGHTS .....</b>	<b>11</b>
<b>APPENDIX B: GLOSSARY.....</b>	<b>13</b>
<b>APPENDIX C: ACRONYMS.....</b>	<b>15</b>
<b>APPENDIX D: DOCUMENT REFERENCES .....</b>	<b>17</b>

## 1. INTRODUCTION

### 1.1 Background

Homeland Security Presidential Directive (HSPD) 12 – *Policy for a Common Identification Standard for Federal Employees and Contractors* establishes “a mandatory, Government-wide standard for secure and reliable forms of identification issued by the Federal Government to its employees and contractors.” [HSPD-12] states that “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. In additional, [HSPD-12] requires “a graduated criteria, from least secure to most secure, to ensure flexibility in selecting the appropriate level of security for each application.”

The secure and reliable form of identification that has been established is the Personal Identity Verification (PIV) Card. Acceptance of PIV Cards between federal government organizations (i.e., inter-organizational trust) is a primary objective of [HSPD-12]. For that objective to be achieved, a baseline level of confidence in both the PIV Card and its issuance process is necessary.

This document articulates the standards and guidelines that define the PIV Card and its issuance process including numerous protective measures specifically designed to establish this baseline level of trust.

### 1.2 Scope

This document highlights the mechanisms currently in place that establish trust in PIV Cards.

### 1.3 Approach

This document identifies the basic elements which enable inter-organizational trust. The elements of trust are discussed in terms of:

- Well-defined standards;
- Compliance regimen that ensures parties adhere to the well-defined standards;
- Relying Party verification whereby relying parties can verify compliance when trusting; and
- Secure components inherent to the PIV Card

### 1.4 Benefits of Inter-organization Trust

Inter-organizational trust of PIV Cards is important because of the benefits it provides to various communities of interest. The following sections describe those benefits.

#### 1.4.1 *Federal Government*

The federal government benefits by:

- Reduction of proprietary, duplicate methodology
- Seamless government-wide interoperability
- Single government-wide technical standard
- Government-wide cost savings and efficiencies

- Contribution to the Homeland Security mission as PIV Cards inherently “enhance security, increase Government efficiency, reduce identity fraud, and protect personal privacy”

#### *1.4.2 Individual Agency*

An individual agency benefit in that:

- Fewer card types for guards and equipment to process, lowering training time and costs
- Easier and faster visitor processing
- Focus on fewer card types enhances ability to become more expert, as well as detect and discern problems and breaches
- Standard card across an agency’s sub-organizations
- Potential for improved access control at both the physical and logical perimeter

#### *1.4.3 End Users*

End Users benefit by:

- Single card access to all federal locations
- Simplified identity verification
- Physical and Logical access on a single card
- Resistance to identity theft

## 2. **ELEMENTS OF TRUST**

This section describes the four related elements of inter-organizational acceptance of PIV Cards. These elements (well-defined standards, compliance regimen that ensures parties adhere to the well-defined standards; relying party verification whereby relying parties can verify compliance when trusting; and Secure components whereby the instruments themselves are secure) are the basis for trust.

### 2.1 **Well-Defined Standards**

The PIV initiative has a suite of standards and guidance documents that define and control critical elements such as card security, physical card construction, card issuance, biometrics, communications, and organization roles and responsibilities.

PIV standards development is an evolving process to further harden against potential threats and mitigate vulnerabilities. In addition, PIV standards support government-wide requirements such as the National Technology Transfer and Advancement Act, and Office of Management and Budget Circular A-119. New and revised documents are vetted by stakeholders, subject matter experts, the vendor community, and other interested parties.

That suite includes standards and guidelines from recognized organizations such as the National Institute of Standards and Technology (NIST), International Standards Organization (ISO), Federal Public Key Infrastructure (FPKI) Policy Authority, American National Standards Institute (ANSI), InterNational Committee for Information Technology Standards (INCITS), International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF), and the Security Industry Association.

### 2.2 **Compliance Regimen**

Compliance with PIV standards and guidance is verified in various ways. Compliance verification is done in a formal, objective, and structured manner against well-defined criteria. Stronger compliance validation enables trust.

The Clinger-Cohen Act (CCA) currently serves as the primary legislative guidance for most executive departments and agencies regarding information technology management. Where the Homeland Security Act is silent, it is anticipated that the relevant provisions of the CCA will apply to the Department of Homeland Security.<sup>2</sup> In addition, congress passed the CCA to instill private-sector IT management best practices in federal agencies<sup>3</sup>. CCA requires programs to use performance based management principles for acquiring IT. These principles include:

- Plan major IT investments;
- Revise processes before investment;
- Enforce accountability for performance;
- Use standards;
- Increase acquisition and incorporation of commercial technology; and
- Use modular contracting.

---

<sup>2</sup> CRS Report to Congress; <http://www.fas.org/sgp/crs/homsec/RS21260.pdf>

<sup>3</sup> CIO News Feature; Allan Holmes; [http://www.cio.com/article/20910/The\\_Clinger\\_Cohen\\_Act](http://www.cio.com/article/20910/The_Clinger_Cohen_Act)

Mechanisms to ensure compliance with CCA in general, and PIV specifically include:

- *FISMA Certification and Accreditation* – ensures compliance with controls that must be followed for all information systems used or operated by a US Government federal agency or by a contractor or other organization on behalf of a US Government agency;
- *FPKIPA Audits* – ensures compliance with FPKI Common Policy;
- *PIV Card Issuance Certification and Accreditation* – ensures PIV Card issuance capability and reliability;
- *PIV Component Validation* – NIST Personal Identity Verification Program (NPIVP) validates PIV components (PIV middleware and PIV Card applications) and their interoperability;
- *Inspector General (IG) Audits* – ensures that their agency is operating efficiently, effectively and legally, and to ensure PIV compliance as necessary;
- *Government Accountability Office (GAO) Audits* – PIV activities are subject to review by the GAO

## 2.3 Relying Party Verification

As federal facilities adopt the required verification technologies, relying parties will evolve trust processing accordingly. These processes will develop over time from visual inspection to real-time certificate validation.

### 2.3.1 Verify Physical PIV Card Integrity

[FIPS 201] requires that the physical PIV Card 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 incorporates one such security feature. Examples of these security features include optical varying structures, optical varying inks, laser etching and engraving, holograms, holographic images, and watermarks.

A security guard can visually inspect the PIV Card security feature(s) to ascertain whether any physical aspect(s) of the card may have been tampered with.

### 2.3.2 Verify Biometrics

The PIV Card displays biometric information on its physical surface (e.g., photograph), and electronically stores biometric information on-board (e.g., fingerprints). The relying party's security guard, PACS or LACS can compare the card holder's biometric(s) with those stored on and/or in the PIV Card.

Physical card security features help protect displayed biometrics, as discussed in Section 2.3.1. Digital signatures help protect on-board biometrics, as discussed by Section 2.3.3.

### 2.3.3 Verify Electronic Signatures

Various on-board data are digitally signed to help detect fraud and tampering. Data items protected by digital signature (directly or indirectly) include, but are not limited to the CHUID, biometric data, the Printed Information Buffer and the Facial Image Buffer. By cryptographically verifying a digital signature, the relying party:

- Authenticates the digital signer (i.e., determine that the digital signature was applied using the expected, corresponding private key); and
- Determines that the digitally signed data has not been tampered with

### 2.3.4 Certificate Path Discovery

As necessary, the relying party can construct a chain of certificates between the FPKI Certification Authority and the PIV Card certificate. Successfully doing so indicates that the issuer of the PIV certificate is trusted.

### 2.3.5 Certificate Validation

X.509 certificates support validation of the associated public key, which is used for, among other things, digital signature verification. The relying party can verify certificate status to determine whether the certificate and its associated public key are valid and usable at that moment in time. Certificate status verification includes checking the following:

- The certificate has not been revoked or suspended; and
- The certificate has not expired

[FIPS 201] and [COMMON] require certificate issuers:

- To revoke a certificate for cause (e.g., card expiration, lost card, stolen card, compromised card); and
- To provide notification of certificate revocation via robust mechanisms such as Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP)

In addition, PIV certificate issuers found to be out of compliance are suspended by the FPKI through revocation of their Common Policy root or Federal Bridge Certification Authority (FBCA) cross certificates. As a result, path discovery will fail, invalidating the PIV Card.

Certificates include an expiration date – typically three (3) years for a PIV certificate. The relying party can check to see if the certificate has expired.

### 2.3.6 Rapid Electronic Authentication

Rapid electronic authentication accesses the PIV Card Issuer (PCI) to determine if the card holder is the same person to whom the PIV Card was issued, in addition to ensuring that the credential is still valid. The PCI provides the relying party with minimum information about the card holder (e.g., name, photograph, credential status). Minimum information protects sensitive information about the individual (e.g., social security number) while helping the relying party make access decisions. Rapid electronic authentication may be accomplished using the contact or contactless interface, a bar code, magnetic stripe, or via manual entry.

## 2.4 Secure Components

PIV Cards incorporate security measures that minimize fraud, tampering, and counterfeiting. Security measures address the full suite of PIV Card use cases (PACS, LACS remote access, LACS local access, visual flash pass). See Appendix A for a list of PIV Card security highlights.

### **3. CONCLUSION**

Trust is the willingness of a relying party to act upon (i.e., rely on) an assertion produced through interaction with a PIV Card. However, trust is always qualified. A relying party may trust one type of interaction in one context (e.g., required confidence level), but not another type of interaction and/or in a different context. Therefore, interaction type and context both matter. The structure of assertions matters as well. Authentication produces an assertion that contains identity information about a Subscriber (e.g., employee, contractor). In addition, transactions may produce attribute assertions. The PIV System is designed to produce trustworthy attribute assertions for the NACI, the facial image, the issuing agency, and the printed information buffer on the card.<sup>4</sup>

The PIV Card, and the overall PIV System, is designed to support all aspects of trust described above. In short, the PIV Card, regardless of the issuing agency, allows any relying party (i.e., any organization) to meet its authentication needs, and possibly attribute needs. This is because of PIV standardization, which, as Section 2 describes, is clearly defined, monitored, and strictly enforced. Standardization ensures robust, reliable, and consistent use by any relying party. There are additional benefits to inter-organization trust of PIV Cards, as discussed in Section 1. Those benefits include, but are not limited to (a) government-wide and individual agency cost savings, (b) contribution to the Homeland Security mission, (c) enhanced authentication problem and breach detection, (d) easier and faster visitor processing, (e) enhanced card holder convenience, and (f) stronger card holder resistance to identity theft.

The value of inter-organizational trust of PIV Cards is significant and compelling – to the federal government as a whole and to individual agencies. It encompasses security enhancement and flexibility, cost savings, expedited processing, enhanced convenience. In the future, the trust element has the potential to seamlessly leverage future PIV innovations and enhancements.

---

<sup>4</sup> Also, possibly, attributes in certificates, as well as optional identifiers, and a small amount of role information such as employee, contractor, and emergency response official. A PIV Card does not provide information about authorizations (although role information just described can be applied to role based access control). In addition, the PIV card-application does not provide information about authorizations, although it might be present elsewhere on the same PIV Card

**APPENDIX A: PIV CARD SECURITY HIGHLIGHTS**

<b>PIV Card Security Highlights</b>
Certain PIV Card data must be cryptographically signed.
The physical PIV Card must include at least one security feature that aids in reducing counterfeiting and resisting tampering attempts, as well as provide visual evidence of tampering.
The PCI must ensure the necessary PKI management functions are supported and implemented in conformance with the security policy objectives mandated in [COMMON].
<p>PIV mandatory and optional cryptographic keys and supporting infrastructure that rely on cryptographic functions must comply with [SP 800-78].</p> <ul style="list-style-type: none"> <li>• This encompasses the PIV Card, infrastructure components that support issuance and management of the PIV Card, and applications that rely on the credentials supported by the PIV Card to provide security services.</li> <li>• The recommendation identifies acceptable symmetric and asymmetric encryption algorithms, digital signature algorithms, and message digest algorithms, and specifies mechanisms to identify the algorithms associated with PIV keys or digital signatures.</li> <li>• Algorithms and key sizes have been selected for consistency with applicable Federal standards and to ensure adequate cryptographic strength for PIV applications.</li> <li>• All cryptographic algorithms employed provide at least 80 bits of security strength.</li> </ul>
<p>All cryptographic modules in the PIV system (both on-card and issuer software) must be validated to FIPS 140-2 with an overall Security Level 2 (or higher).</p> <ul style="list-style-type: none"> <li>• All PIV cryptographic keys are generated within a FIPS 140-2 validated cryptomodule</li> <li>• In addition to an overall validation of Level 2, the PIV Card provides Level 3 physical security to protect the PIV private keys in storage.</li> </ul>
Systems within the PIV infrastructure must utilize security controls described in [SP 800-53].
All cryptographic operations using PIV keys must be performed on-card.
Certain PIV keys (e.g., authentication key, digital signature key) must be generated on-card, and cannot be exported.
Certain PIV Card features (e.g., PIV authentication key, PIV digital signature key) must only be used in the more secure contact interface environment.
All FIPS 201 mandatory information printed on the PIV Card is duplicated on the chip in the Printed Information Buffer. The Security Object enforces integrity of this information according to the issuer. This provides specific protection that the PIV Card information must match the printed information, mitigating alteration risks on the printed media.
<p>Security architecture software in the integrated circuit chip (ICC) applies security policy to all card commands thereby ensuring that the prescribed data policies for the card applications are enforced. This includes:</p> <ul style="list-style-type: none"> <li>• Access control rule</li> <li>• Security status</li> <li>• Authentication of an individual (e.g., knowledge of a PIN)</li> </ul>
Card production may be accomplished either centrally or at a distributed issuer facility, provided security and quality control objectives for card stock management are fully met.

**PIV Card Security Highlights**

Biometric matches are required to obtain or update a PIV Card. This includes:

- The PCI performs a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record. Only on successful match is the PIV Card released to the applicant
- Upon PIV Card reissuance or renewal, the PCI verifies the individual with a 1:1 biometric match against the IDMS record
- Upon PIN set or reset, before the PIV Card is provided back to the card holder, the PCI ensures that the card holder's biometric matches the stored biometric on the PIV Card.

**APPENDIX B: GLOSSARY**

Term	Definition
Accreditation	Formal approval of an entity to assess PIV Card issuing agencies on behalf of the federal government.
Certification	Formal process of making certain that an individual, organization, or system is qualified in terms of a particular set of requirements. Certification are often fostered or supervised by some certifying agent, such as a professional association or organization.
Compliance	Acting according to specified standards and guidance.
Contact PIV Card	Dedicated Integrated Circuit Chip (ICC) interface to allow a PIV Card to be inserted into a card reader for processing. The ICC makes contact with electrical connectors that can read information from the chip and write information back.
Contactless PIV Card	Dedicated Integrated Circuit Chip (ICC) interface to allow a PIV Card to be processed by a card reader without having to insert the PIV Card into the reader. The ICC communicates with the card reader through Radio-frequency identification (RFID) induction technology. These cards require only close proximity to an antenna to complete transaction. They are often used when transactions must be processed quickly or hands-free.
Credential	Evidence attesting to one's right to credit or authority; for purposes of this Trust Model, it is the PIV Card and data elements associated with an individual that authoritatively binds an identity (and, optionally, additional attributes) to that individual.
Guidance	Direction or advice as to a decision or course of action.
National Voluntary Laboratory Accreditation Program (NVLAP)	All of the tests under NPIVP are handled by third-party test facilities that are accredited as cryptographic module test laboratory by the National Voluntary Laboratory Accreditation Program (NVLAP) and have extended their scope of testing to include PIV Card application and PIV middleware test methods.
NIST Personal Identity Verification Program (NPIVP)	The National Institute of Standards and Technology has established the NIST Personal Identity Verification Program (NPIVP) to validate Personal Identity Verification (PIV) components required by Federal Information Processing Standard (FIPS) 201.
Personal Identity Verification (PIV)	The term designated in FIPS 201 for the processes and technologies involved in (a) identification: verifying the identity of a Federal employee or contractor at the time of initial identification and enrollment into a Federal agency's identity management system, and (b) authentication: verifying the identity of the employee or contractor for purposes of physical and information systems access control.

Term	Definition
PIV Card	A physical artifact (e.g., identity card, “smart” card) issued to an individual that contains stored identity credentials (e.g., photograph, cryptographic keys, digitized fingerprint representation) so that the claimed identity of the card holder can be verified against the stored credentials by another person (human readable and verifiable) or an automated process (computer readable and verifiable).
PIV Card Issuer (PCI)	An authorized identity card creator that procures FIPS-approved blank identity cards, initializes them with appropriate software and data elements for the requested identity verification and access control application, personalizes the cards with the identity credentials of the authorized subjects, and delivers the personalized cards to the authorized subjects along with appropriate instructions for protection and use.
PIV Card Issuing Agency	The organization that is issuing the PIV Card to an Applicant. Typically this is an organization for which the Applicant is working.
Relying Party	An organization that trusts a PIV Card for purposes of authenticating an individual for physical access (e.g., to a building) and/or logical access (e.g., to an IT system).
Standard	A published statement on a topic specifying the characteristics, usually measurable, that must be satisfied or achieved to comply with the standard.
Trust	Belief (i.e., presumption) that the PIV Card has been issued in accordance with a Relying Agency’s expectations and needs. Trust allows a Relying Agency to process the PIV Card (via PACS, LACS, and/or flash pass) with an applicable level of confidence.
Validation	The process of demonstrating that the system under consideration meets in all respects the specification of that system.

**APPENDIX C: ACRONYMS**

Acronym	Definition
AIA	Authority Information Access
ANSI	American National Standards Institute
C&A	Certification and Accreditation
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Card Holder Unique Identifier
CMS	Cryptographic Message Syntax
CMTC	Card Management System to the Card
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CSE	Communications Security Establishment
CTC	Card holder to the Card
CTE	Card holder to an External Entity
FASC-N	Federal Agency Smart Credential – Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act of 2002
GAO	Government Accountability Office
HSPD	Homeland Security Presidential Direct
ICAO	International Civil Aviation Organization
ICC	Integrated Circuit Chip
ID	Identification
IDMS	Identity Management System
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
INCITS	InterNational Committee for Information Technology Standards
ISO	International Standards Organization
IT	Information Technology
LACS	Logical Access Control System
NACI	National Agency Check and Inquiries
NIST	National Institute of Standards and Technology
NPIVP	NIST Personal Identity Verification Program
NVLAP	National Voluntary Laboratory Accreditation Program
OCSP	Online Certificate Status Protocol
OMB	Office of Management and Budget
PACS	Physical Access Control System

---

Acronym	Definition
PCI	PIV Card Issuer
PIN	Personal Identification Number
PIV	Personal Identity Verification
RFC	Request for Comment
RFID	Radio Frequency Identification
SP	Special Publication

## **APPENDIX D: DOCUMENT REFERENCES**

This appendix highlights documents directly or indirectly relevant to PIV Card design, issuance, maintenance, and use. It is not intended to be a complete list. Compliance with these and other relevant documents enables inter-organization trust of PIV Cards.

### **Executive and Legislative**

- [Circular A-119] Federal Participation in the Development and Use of Voluntary Consensus Standards and in Conformity Assessment Activities  
<http://www.whitehouse.gov/omb/circulars/a119/a119.html>
- [Circular A-123] Management's Responsibility for Internal Control; Office of Management and Budget  
[http://www.whitehouse.gov/omb/circulars/a123/a123\\_rev.html](http://www.whitehouse.gov/omb/circulars/a123/a123_rev.html)
- [FISMA] Federal Information Security Management Act  
<http://csrc.nist.gov/sec-cert/>
- [HSPD-12] Policy for a Common Identification Standard for Federal Employees and Contractors  
<http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html>
- [NTTAA] National Technology Transfer and Advancement Act of 1995  
[http://standards.gov/standards\\_gov/nttaa.cfm](http://standards.gov/standards_gov/nttaa.cfm)

### **OMB Memorandum**

- [OMB M-03-22] OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Office of Management and Budget (OMB) Memorandum M-03-22  
<http://www.whitehouse.gov/omb/memoranda/m03-22.html>
- [OMB M-04-04] E-Authentication Guidance for Federal Agencies, Office of Management and Budget (OMB) Memorandum M-04-04  
<http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf>
- [OMB M-05-24] Implementation of Homeland Security Presidential Directive (HSPD)  
<http://www.whitehouse.gov/omb/memoranda/fy2005/m05-24.pdf>
- [OMB M-06-18] Acquisition of Products and Services for Implementation of HSPD-12  
<http://www.whitehouse.gov/omb/memoranda/fy2006/m06-18.pdf>

**FPKIPA Policies and Profiles**

- [COMMON] X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework, Version 2.0, November 1, 2004.  
<http://www.cio.gov/ficc/documents/CommonPolicy.pdf>
- [PROF] X.509 Certificate and CRL Profile for the Common Policy, Version 1.1, July 8, 2004.  
<http://www.cio.gov/ficc/documents/CertCRLprofileForCP.pdf>

**NIST Standards**

- [FIPS 140-2] Security Requirements for Cryptographic Modules  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 186-3] Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000), to be published  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 180-2] Secure Hash Standard (SHS)  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 196] Entity Authentication Using Public Key Cryptography  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 197] Advanced Encryption Standard (AES), November 2001  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 198-1] The Keyed-Hash Message Authentication Code (HMAC)  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 199] Standards for Security Categorization of Federal Information and Information Systems  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 200] Minimum Security Requirements for Federal Information and Information Systems  
<http://www.itl.nist.gov/fipspubs/by-num.htm>
- [FIPS 201-1] NIST FIPS 201-1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, NIST, March 2006.  
<http://www.itl.nist.gov/fipspubs/by-num.htm>

**Joint NIST/ANSI Standard**

- [SP 500-245] Data Format for the Interchange of Fingerprint, Facial, & Scar Mark & Tattoo (SMT) Information, ANSI/NIST-ITL 1-2000  
[ftp://sequoyah.nist.gov/pub/nist\\_internal\\_reports/sp500-245-a16.pdf](ftp://sequoyah.nist.gov/pub/nist_internal_reports/sp500-245-a16.pdf)

**NIST Guidance**

- [SP 800-15] Minimum Interoperability Specification for PKI Components (MISPC), V. 1  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-18] Guide for Developing Security Plans for Federal Information Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-25] Federal Agency Use of Public Key Technology for Digital Signatures and Authentication  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-26] Security Self-Assessment Guide for Information Technology Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-30] Risk Management Guide for Information Technology Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-37] Guide for the Security Certification and Accreditation of Federal Information Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-38C] Recommendation for Block Cipher Modes of Operation: the CCM Mode for Authentication and Confidentiality  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-47] Security Guide for Interconnecting Information Technology Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-53] Recommended Security Controls for Federal Information Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-53A] Guide for Assessing the Security Controls in Federation Information Systems  
<http://csrc.nist.gov/publications/nistpubs/>

- 
- [SP 800-56] Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-57] Recommendation for Key Management  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-59] Guideline for Identifying an Information System as a National Security System  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-60] Guide for Mapping Types of Information and Information Systems to Security Categories  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-67] Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-73] Interfaces for Personal Identity Verification  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-76-1] Biometric Data Specification for Personal Identity Verification  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-78-1] Cryptographic Standards and Key Sizes for Personal Identity Verification  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-79] Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-79Q&A] Questions and Answers about the Certification and Accreditation of PIV Card Issuing Organizations  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-79Q&A Part2] Questions and Answers Regarding the Certification and Accreditation of PIV Card Issuing Organizations  
<http://csrc.nist.gov/publications/nistpubs/>
-

- [SP 800-85A] PIV Card Application and Middleware Interface Test Guidelines (SP800-73 compliance)  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-85B] PIV Data Model Conformance Test Guidelines  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-87] Codes for the identification of Federal and Federally-assisted Organizations  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-90] Recommendation for Random Number Generation Using Deterministic Random Bit Generators  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-96] PIV Card / Reader Interoperability Guidelines  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-98] Guidelines for Securing Radio Frequency Identification (RFID) Systems  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-100] Information Security Handbook: A Guide for Managers  
<http://csrc.nist.gov/publications/nistpubs/>
- [SP 800-104] A Scheme for PIV Visual Card Topography  
<http://csrc.nist.gov/publications/nistpubs/>

### **NIST Testing**

- [NPIVP] National Institute of Standards and Technology has established the NIST Personal Identity Verification Program (NPIVP)  
<http://csrc.nist.gov/npivp/>
- [NVLAP] National Voluntary Laboratory Accreditation Program (NVLAP)  
<http://csrc.nist.gov/npivp/>

### **NIST Overviews**

- [PIV Update] Personal Identity Verification Program Power Point Presentation, William C. Barker, NIST  
<http://csrc.nist.gov/npivp/NPIVPWorkshopPresentations/CBarker.ppt>

**SmartGov Guidance**

[SCEPACS] Technical Implementation Guidance: Smart Card Enabled Physical Access Control Systems  
<http://www.smart.gov/iab/documents/PACS.pdf>

**ANSI Standards**

[ANSI X.9.31] RSA Digital Signatures

[ANSI X.9.62] Elliptic Curve Digital Signature

[ANSI X.9.82] Random Number Generation

**IEC Standards**

[IEC 61966-2-1:1999] Multimedia systems and equipment - Colour measurement and management - Part 2-1: Colour management - Default RGB colour space - sRGB

**IETF Standards**

[RFC 2119] Key Words for Use in RFCs to Indicate Requirement Levels, March, 1997  
<http://www.ietf.org/rfc/rfc2119.txt>

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

[RFC 3279] Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation Lists (CRL) Profile, April 2002.  
<http://www.faqs.org/rfcs/rfc3279.html>

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

[RFC 3447] Jonsson, J., and B. Kaliski, "PKCS #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003  
<http://www.faqs.org/rfcs/rfc3447.html>

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

**INCITS Standards**

- [INCITS 378-2004] American National Standard for Information Technology - Finger Minutiae Format for Data Interchange
- [INCITS 381-2004] American National Standard for Information Technology - Finger Image-Based Data Interchange Format
- [INCITS 385-2004] American National Standard for Information Technology - Face Recognition Format for Data Interchange

**ISO Standards**

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

**Joint ANSI/INCITS Standards**

- [ANSI/INCITS 322] Information Technology, Card Durability Test Methods, ANSI, 2002.
- [ANSI/INCITS M1-040211] Biometric Profile—Interoperability and Data Interchange—Biometrics-Based Verification and Identification of Transportation Workers, ANSI, April 2004.

**Joint ISO/IEC Standards**

- [ISO/IEC 10373] Identification Cards—Test Methods. Part 1—Standard for General Characteristic Test of Identification Cards, ISO, 1998. Part 3—Standard for Integrated Circuit Cards with Contacts and Related Interface Devices, ISO, 2001. Part 6—Standard for Proximity Card Support in Identification Cards, ISO, 2001
- [ISO/IEC 14443-1:2000] Identification cards - Contactless integrated circuit(s) cards – Proximity cards - Part 1: Physical Characteristics
- [ISO/IEC 14443-1:2000] Identification Cards—Contactless Integrated Circuit(s) Cards—Proximity Cards, ISO, 2000
- [ISO/IEC 14443-2:2001] Identification cards - Contactless integrated circuit(s) cards – Proximity cards - Part 2: Radio frequency power and signal interface  
AMENDMENT 1: Bit rates of fc/64, fc/32 and fc/16
- [ISO/IEC 14443-3:2001] Identification cards – Contactless integrated circuit(s) cards – Proximity cards Part 3: Initialization and anticollision. AMENDMENT 1: Bit rates of fc /64, fc /32 and fc /16, AMENDMENT 3: Handling of reserved field and values

- [ISO/IEC 14443-4:2001] Identification cards – Contactless integrated circuit(s) cards – Proximity cards Part 4: Transmission Protocol AMENDMENT 1: Handling of reserved fields and values
- [ISO/IEC 19795:2005] Information Technology — Biometric Performance Testing and Reporting — Part 4: Interoperability Performance Testing
- [ISO/IEC 7810:2003] Identification Cards—Physical Characteristics, ISO, 2003
- [ISO/IEC 7816] Information technology — Identification cards — Integrated circuit(s) cards with Contacts, (Parts 4, 5, 6, 8, and 9)]
- [ISO/IEC 7816] Identification Cards—Integrated Circuits with Contacts, Parts 1-6, ISO
- [ISO/IEC 7816-3:1997] Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols
- [ISO/IEC 7816-3:1997] Information technology - Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols AMENDMENT 1: Electrical characteristics and class indication for integrated circuit(s) cards operating at 5 V, 3 V and 1.8 V
- [ISO/IEC 8824-2:2002] Information technology -- Abstract Syntax Notation One (ASN.1): Information object specification
- [ISO/IEC 8825-1:2002] Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)

### **PC/SC Workgroup Standards**

- [PC/SC Spec] PC/SC - Interoperability Specification for ICCs and Personal Computer Systems Part 2. Interface Requirements for Compatible IC Cards and Readers, Revision 2.01.02, September 2005  
[http://www.pcscworkgroup.com/specifications/files/pcsc2\\_v2.01.01.pdf](http://www.pcscworkgroup.com/specifications/files/pcsc2_v2.01.01.pdf)