X-Sieve: CMU Sieve 2.2
Subject: IAB Final Comments in the Required Format for FIPS 201 comments to NIST
To: james.dray@nist.gov, wbarker@nist.gov, Bob_Donelson@blm.gov,
branstad@nist.gov
Cc: "'cierianthony@yahoo.com'" <cierianthony@yahoo.com>,
"'daryl.hendricks@gsa.gov'" <daryl.hendricks@gsa.gov>,
"Gallagher, Deborah S.,,DMDCEAST" <Deborah.Gallagher@osd.pentagon.mil>,
"'fred.catoe@mail.va.gov'" <fred.catoe@mail.va.gov>,
"Gilson, Bob R, , DMDCEAST" <irving.Gilson@osd.pentagon.mil>,
"'jepagan@state.pa.us'" <jepagan@state.pa.us>,
"'Jim.Zok@marad.dot.gov'" <Jim.Zok@marad.dot.gov>,
"'Joe.Broghamer@dhs.gov'" <Joe.Broghamer@dhs.gov>,
"'Lolie.Kull@dhs.gov'" <Lolie.Kull@dhs.gov>,
"Van Mullekom, Mary P,, DMDCEAST" <Mary.VanMullekom@osd.pentagon.mil>,
"Butler, Michael P.,,DMDCEAST" <Michael.Butler@osd.pentagon.mil>,
"'rick.uhrig@comcast.net'" <rick.uhrig@comcast.net>,
"Van Spyk, Robert P,,DMDCWEST" <robert.vanspyk@osd.pentagon.mil>,
"'stevehoward@cox.net'" <stevehoward@cox.net>,
"'Sulakma@state.gov'" <Sulakma@state.gov>,
"'thomas.casey@gsa.gov'" <thomas.casey@gsa.gov>,
"'tim.w.baldridge@nasa.gov'" <tim.w.baldridge@nasa.gov>,
"'trung.nguyen@do.treas.gov'" <trung.nguyen@do.treas.gov>,
"Boggess, Bill F,,DMDCWEST" <william.boggess@osd.pentagon.mil>,
"Gilson, Bob R, , DMDCEAST" <irving.Gilson@osd.pentagon.mil>
X-Mailer: Lotus Notes Release 5.0.11 July 24, 2002
From: Bob_Donelson@blm.gov
Date: Wed, 22 Dec 2004 17:29:36 -0500
X-MIMETrack: Serialize by Router on LMNI11/BLM/DOI(Release 6.0.3|September 26, 2003) at
12/22/2004 03:25:53 PM
X-MailScanner:
X-MailScanner-From: bob_donelson@blm.gov

Jim and Curt

The following are the final comments from the IAB in your required format for FIPS 201. in addition we are providing a cover letter of general explanation, a proposed rewrite of the FIPS and a Power Point Presentation outlining the major areas of change.

(See attached file: 2004-12-21 IAB FIPS 201 comments submission.xls)

(See attached file: 2004-12-21 IAB FIPS 201 Cover Letter Final.doc)(See attached file: 2004-12-21 IAB FIPS 201 Summary Changes.ppt)(See attached file: 2004-12-21 IAB FIPS 201_Version 2_Final.doc)


2004-12-21 IAB FIPS 201 comments submission.xls


2004-12-21 IAB FIPS 201 Cover Letter Final.doc


2004-12-21 IAB FIPS 201 Summary Changes.ppt


2004-12-21 IAB FIPS 201_Version 2_Final.doc

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section, Annex, etc. and Page Nbr	Comment(Include rationale for comment)	Proposed change
1	IAB	Bob Donelson	G	Section 1	Minor edits. Change references of "computer" to "logical"	See IAB Recommended Revisions to FIPS 201
2	IAB	Bob Donelson	G	Section 1.1	Expanded, tied back to HSPD-12, combined with scope.	See IAB Recommended Revisions to FIPS 201
3	IAB	Bob Donelson	G	Section 1.2	Combined with previous section.	See IAB Recommended Revisions to FIPS 201
4	IAB	Bob Donelson	G	Section 1.3	Updated to reflect new organization.	See IAB Recommended Revisions to FIPS 201
5	IAB	Bob Donelson	G	Section 2	Expanded to reflect PIV-I compliance is mandated by Oct 2005; Tied reference to SP 800-73	See IAB Recommended Revisions to FIPS 201
6	IAB	Bob Donelson	G	Section 2.1	Augmented four HSPD-12 objectives with six functional objectives. Deleted statement specifying PIV-II content Added Use Case and Requirements • Registration • Validation • Physical Access • Logical Access Added new subsection 2.1.1 Definitions Added new subsection 2.1.2 Scope of PIV-I	This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
7	IAB	Bob Donelson	G	Section 2.2	Replaced old process with a new one; Added a figure; Defined roles, components, identity proofing, issuance requirements and workflow.	This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
8	IAB	Bob Donelson	G	Section 2.2.1	Change title, dropped "of New Employees and Contractors" and made section apply to both new and current employees Deleted entire notion of Position Sensitivity Level Explicitly allowed centralized issuance Specified electronic aspects of enrollment package Mandated an Identity Management System (IDMS) that includes a one-to-many search for alias checking Added a detailed breakdown in additional subsections • Employer/Sponsor • PIV Application Process • PIV Enrollment Process • Identity Verification Process • Card Production, Activation, and Issuance • Suspension, Revocation and Destruction	Focus on identity and chain of trust, not trustworthiness. This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
9	IAB	Bob Donelson	G	Section 2.2.2	This section has been changed to "Re-Issuance to Current PIV Credential Holders"	See IAB Recommended Revisions to FIPS 201
10	IAB	Bob Donelson	G	Section 2.2.3	Minor edit. Change "background" to "1:many" check.	This is consistent with identity rather than trustworthiness. See IAB Recommended Revisions to FIPS 201
11	IAB	Bob Donelson	G	Section 2.2.4	Minor edit	See IAB Recommended Revisions to FIPS 201
12	IAB	Bob Donelson	G	Section 2.3	Incorporated above in "Card Production, Activation, and Issuance"	See IAB Recommended Revisions to FIPS 201
13	IAB	Bob Donelson	G	Section 3	Section 3 and all subordinate subsections were removed. These were informative and did not add any requirements to the standard. This information may be included in a separate rationale or guidance document.	See IAB Recommended Revisions to FIPS 201
14	IAB	Bob Donelson	G	Section 4	Substantially reorganized and re-titled this section and subordinate subsections:	See IAB Recommended Revisions to FIPS 201
15	IAB	Bob Donelson	G	Section 4.1	Minor edits. Reformatted	See IAB Recommended Revisions to FIPS 201
16	IAB	Bob Donelson	G	Section 4.1.1	Deleted in its entirety. Procurement requirements, perhaps more appropriate for printer and inks.	See IAB Recommended Revisions to FIPS 201
17	IAB	Bob Donelson	G	Section 4.1.2	Reformatted. Added reference to expanded physical security requirements in SP 800-73	See IAB Recommended Revisions to FIPS 201

Cmt #	Org.	Point of Contact	Type (G, E, T)	Section, Annex, etc. and Page Nbr	Comment (include rationale for comment)	Proposed change
18	IAB	Bob Donelson	G	Section 4.1.3	Largely deleted. Requirements to NOT emboss, punch, or affix with decals promoted one level	See IAB Recommended Revisions to FIPS 201
19	IAB	Bob Donelson	G	Section 4.1.4	Renamed "PIV Credential Data" with 3 major subsections: • Graphical Data • ICC Data • Machine Readable Data Summarize free text in succinct table format Require that all data elements will conform to PDMF as specified in SP 800-73	See IAB Recommended Revisions to FIPS 201
20	IAB	Bob Donelson	G	Section 4.1.5	Subsumed into table above References PDMF in SP 800-73	See IAB Recommended Revisions to FIPS 201
21	IAB	Bob Donelson	G	Section 4.1.5.1	Deleted. Relegated to SP 800-73	See IAB Recommended Revisions to FIPS 201
22	IAB	Bob Donelson	G	Section 4.1.5.2	The PIV card must be activated to perform privileged operations. The PIV card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system. Cardholder authentication is described in Section 4.1.6.1 and Card Management system authentication is described in Section 4.1.6.2.	See IAB Recommended Revisions to FIPS 201
23	IAB	Bob Donelson	G	Section 4.1.6	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules.	See IAB Recommended Revisions to FIPS 201
24	IAB	Bob Donelson	G	Section 4.1.6.1	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules.	See IAB Recommended Revisions to FIPS 201
25	IAB	Bob Donelson	G	Section 4.2	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules.	See IAB Recommended Revisions to FIPS 201
26	IAB	Bob Donelson	G	Section 4.2.1	Deleted. Relegated to SP 800-73 PDMF and Access Control Rules. The TIG PACS version 2.2 is a normative reference to SP 800-73 and the PDMF. Specifically. Position Sensitivity Level and Expiration Date will NOT be added	See IAB Recommended Revisions to FIPS 201
27	IAB	Bob Donelson	G	Section 4.2.2	The TIG PACS version 2.2 is a normative reference to SP 800-73 and the PDMF. Specifically. Asymmetric signature field in CHUID conforms with ICAO 9303 MRTD PKI technical guidance.	See IAB Recommended Revisions to FIPS 201
28	IAB	Bob Donelson	G	Section 4.3	Elevated to a major section. Reformatted content Removed narrative text and extracted explicit requirements.	See IAB Recommended Revisions to FIPS 201
29	IAB	Bob Donelson	G	Section 4.4	Elevated to major section Kept mandatory biometric data to be collected and retained Moved technical specifications to SP 800-73 Reorganized subordinate sections to: • Fingerprint Biometric • Facial Biometric • PIV Registration [Biometric Enrollment] and Issuance	See IAB Recommended Revisions to FIPS 201
30	IAB	Bob Donelson	G	Section 4.4.1	Minor edits. Deleted descriptive text. Specified biometric data quality, format, integrity, and confidentiality will be described in SP 800-73.	See IAB Recommended Revisions to FIPS 201
31	IAB	Bob Donelson	G	Section 4.4.2	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
32	IAB	Bob Donelson	G	Section 4.4.3	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
33	IAB	Bob Donelson	G	Section 4.4.4	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
34	IAB	Bob Donelson	G	Section 4.4.5	Reformatted. Added statement that no algorithmic facial recognition systems are mandatory if fingerprint is not available.	See IAB Recommended Revisions to FIPS 201

Cmt #	Org	Point of Contact	Type (G, E, T)	Section, Annex, etc. and Page Nbr	Comment (include rationale for comment)	Proposed change
35	IAB	Bob Donelson	G	Section 4.4.5.1	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
36	IAB	Bob Donelson	G	Section 4.4.5.2	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
37	IAB	Bob Donelson	G	Section 4.4.5.3	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
38	IAB	Bob Donelson	G	Section 4.4.5.4	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
39	IAB	Bob Donelson	G	Section 4.4.5.5	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
40	IAB	Bob Donelson	G	Section 4.4.5.6	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
41	IAB	Bob Donelson	G	Section 4.4.5.7	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
42	IAB	Bob Donelson	G	Section 4.4.5.8	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
43	IAB	Bob Donelson	G	Section 4.4.6	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
44	IAB	Bob Donelson	G	Section 4.5	Elevated to major section. Reference to SP 800-73 for additional card reader specifications	See IAB Recommended Revisions to FIPS 201
45	IAB	Bob Donelson	G	Section 4.5.1	Reformatted with minor edits	See IAB Recommended Revisions to FIPS 201
46	IAB	Bob Donelson	G	Section 4.5.2	Reformatted with minor edits	See IAB Recommended Revisions to FIPS 201
47	IAB	Bob Donelson	G	Section 4.5.3	Deleted. Relegated to Implementation Guidance	See IAB Recommended Revisions to FIPS 201
48	IAB	Bob Donelson	G	Section 5	Deleted and all subsections are deleted. Relegated to chapter 2 and SP 800-73.	See IAB Recommended Revisions to FIPS 201
49	IAB	Bob Donelson	G	Section 5.1	Deleted and all subsections are deleted. Relegated to PIV-I, section 2 and SP 800-73.	See IAB Recommended Revisions to FIPS 201
50	IAB	Bob Donelson	G	Section 5.1.1	Deleted and all subsections are deleted. Relegated to PIV-I, section 2 and SP 800-73. Registration Database one component of the IDMS.	See IAB Recommended Revisions to FIPS 201
51	IAB	Bob Donelson	G	Section 5.1.2	Deleted. Relegated to SP 800-73.	See IAB Recommended Revisions to FIPS 201
52	IAB	Bob Donelson	G	Section 5.2	Deleted and all subsections are deleted. Moved to PIV-I, section 2 and Implementation Guidance.	See IAB Recommended Revisions to FIPS 201
53	IAB	Bob Donelson	G	Section 5.2.1.1	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
54	IAB	Bob Donelson	G	Section 5.2.1.2	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
55	IAB	Bob Donelson	G	Section 5.2.1.3	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
56	IAB	Bob Donelson	G	Section 5.2.2	Moved to PIV-I, section 2.	See IAB Recommended Revisions to FIPS 201
57	IAB	Bob Donelson	G	Section 5.2.3	This and all subordinate sections have been deleted. PKI and Certificate management and policy for logical access control are within the purview of the FICC and out of scope for this document.	See IAB Recommended Revisions to FIPS 201
58	IAB	Bob Donelson	G	Section 5.2.3.1	Deleted.	See IAB Recommended Revisions to FIPS 201
59	IAB	Bob Donelson	G	Section 5.2.3.2	Deleted.	See IAB Recommended Revisions to FIPS 201
60	IAB	Bob Donelson	G	Section 5.2.3.3	Deleted.	See IAB Recommended Revisions to FIPS 201
61	IAB	Bob Donelson	G	Section 5.2.3.4	Deleted.	See IAB Recommended Revisions to FIPS 201
62	IAB	Bob Donelson	G	Section 5.2.3.5	Deleted.	See IAB Recommended Revisions to FIPS 201
63	IAB	Bob Donelson	G	Section 5.2.3.6	Deleted.	See IAB Recommended Revisions to FIPS 201

Cmt #	Org	Point of Contact	Type (G, E, T)	Section, Annex, etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
64	IAB	Bob Donelson	G	Section 5.2.4	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
65	IAB	Bob Donelson	G	Section 5.2.4.1	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
66	IAB	Bob Donelson	G	Section 5.2.4.2	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
67	IAB	Bob Donelson	G	Section 5.2.4.3	Deleted. Position Sensitivity Level is no longer a part of the PIV.	See IAB Recommended Revisions to FIPS 201
68	IAB	Bob Donelson	G	Section 5.2.5	Moved to PIV-I, section 2	See IAB Recommended Revisions to FIPS 201
69	IAB	Bob Donelson	G	Section 6	Content in this section was informative. It is replaced by appropriate graduated criteria, use cases, and implementation guidance per OMB	See IAB Recommended Revisions to FIPS 201
70	IAB	Bob Donelson	G	Annexes A-D	Annexes A through D provide significant guidance and are removed in favor the re-organized FIPS 201. Implementation Guidance, Certification, and Accreditation must be specified through OMB implementation and acquisition guidance.	See IAB Recommended Revisions to FIPS 201
	Detailed Comments Follow					
71	IAB	Bob Donelson	G	Throughout, including D1, p v, par 8; D1, p vi, par 10; D1, p ix (x2) D1.1.2 p 2 (x2); D1.2.2.1 p 5 (x2), p 6 (x4); D1.3 p 10; D1.1.3.1 p 10; D1.3.2.1 p 11; D1.4.2.1 p 25 (x5); D1.4.4.1 p 30 (x2); D1.5.2.1.1 p 41 (x4), p 42 (x2); D1.5.2.4.3 p 47 (x3); D1.6.1.2 p 51; D1.6.1.3 p 52; D1.E.1 p 76 (x3), p 77	**Position Sensitivity Level (PSL).** PSL measures the "trustworthiness" of a claimed identity. HSPD-12's mandate and scope is limited to establishing the claimed identity and not its trustworthiness. The two differ substantially. PSL introduces a number of issues: (1) the possibility that some employees with verified identity are not issued PIV cards (in apparent contradiction to HSPD-12), (2) it encroaches on the authority of departments and agencies to determine their own processes and procedures for determining trustworthiness and granting clearances, (3) it will be useful only if clearance schemes across the federal government are unified. This seems to be unlikely and out of scope (4) the level naming scheme of 1, 2, 3, and 4 uses names that are not meaningful or instructive.	1. Delete all references of Position Sensitivity Level. 2. Eliminate all trustworthiness checks 3. Eliminate PSL field from the CHUID These changes have been incorporated in the IAB Recommended Revisions to FIPS 201
72	IAB	Bob Donelson	G	Not Present	**Graduated Criteria.** HSPD-12 mandates the inclusion of graduated criteria, from least secure to most secure. There are a number of areas where graduated criteria could effectively be specified: 1. Resistance to Tampering & Counterfeiting o Graphical o Electrical 2. Electronic Authentication o PIV Authentication o Cardholder Authentication	Add graduated criteria for each of: 1. Graphical Resistance 2. Electrical Resistance 3. PIV Authentication 4. Cardholder Authentication These changes have been incorporated in the IAB Recommended Revisions to FIPS 201, Section 7

Cmt #	Org	Point of Contact	Type (G, E, T)	Section/Annex/etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
73	IAB	Bob Donelson	G	D1.4.1.4, p 19-22	**Uniform PIV Appearance**. FIPS 201 PUBLIC Draft does NOT adequately specify a uniform appearance of PIVs. Recognizable, uniform appearance of PIVS across Federal issuers is needed to meet HSPD-12's mandate for "Secure and reliable" – it will allow minimally trained personnel to recognize each PIV as a Federally issued credential. To achieve a uniform appearance the following must be addressed: • Background Color and Pattern. This needs to be clearly specified, together with any allowed variations. • Zone Location and Size. Each zone must be specified to an adequate degree of precision (say hundredths of an inch.) Locations should be specified relative to a fixed reference (e.g. from top left corner) • Fonts & Font Sizes. These must need specified more tightly, especially on the front of the card. The PD merely specifies minimum size. To achieve a common look, font size variability must be limited as much as possible. Also, for a few optional fields, font type and size have been omitted entirely. • Additional Printing. A clear policy statement on what additional printing or graphics an issuer may a	Clearly and completely specify: • Background color and pattern, along with any allowed variations. • Location and size of each zone to an adequate degree of precision (hundredths of an inch.) Locations should be specified relative to a fixed reference (e.g. from top left corner) • Font sizes precisely, not merely as minimums. • Specify font type and size for optional fields that has been omitted. • Policy statement on additional printing and graphics an issuer may add. If possible, provide as an exhaustive list of what is allowed Placeholders for this information have been incorporated in the IAB Recommended Revisions to FIPS 201, Section 3.4
74	IAB	Bob Donelson	G	D1.4.1.2, p 17	**Uniform Graphical Security Features**. The FIPS 201 specifications for a graphical security feature – a tri-modal or bi-modal OVD or OVI are completely inadequate for providing any uniformity of this feature. Without uniformity the security features will be completely ineffective, as moderately trained individuals will have little chance of differentiating between legitimate and counterfeit PIV.	Detailed specifications for human verifiable security features must be defined and published. Forensic security features must be defined but should NOT be published in widely available public documents. (Reference how closely held the security feature specifications are for passports and printed currency) A uniform security feature should be specified outside of the FIPS 201 standard.
75	IAB	Bob Donelson	G	D1.4.1.2, p 17	**Adequate Graphical Security Features.** FIPS 201 requires only a single graphical security feature – the tri-modal or bi-modal OVD or OVI. This is inadequate protection against counterfeiting. A host of technologies are available - including holographic overlay, guilloche, very fine line, micro printing, laser engraving, laser printing, UV inks, hidden word, digital watermarking and laminate glues to name a few. To meet the HSPD-12 mandate to "be strongly resistant to … counterfeiting", much stronger specification of a uniform set of anti-counterfeiting techniques is required.	Detailed specifications for human verifiable security features must be defined and published. Forensic security features must be defined but NOT be published in widely available public documents. (Reference how closely held the security feature specifications are for passports and printed currency) An adequate set of additional security features should be specified outside of the FIPS 201 standard. The need for adequate security features has been acknowledged in the IAB Recommended Revisions to FIPS 201, Section 7.1.1.

Cmt #	Org	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(include rationale for comment)	Proposed change
76	IAB	Bob Donelson	G	D1.2.3, p 7	**Central Issuance.** 201 PUBLIC Draft does not allow central issuance: "The Issuing Authority shall photograph the Applicant at the time of Issuance and retain a file copy of the image. The identity credential shall then be personalized for the Applicant." Central issuance is more cost-effective and provides much stronger lifecycle security (in several respects, particularly from the perspective of protecting blank cardstock.)	Allow central issuance for PIV cards. This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5
77	IAB	Bob Donelson	G	Omitted Item	**Unprotected Blank Cardstock.** Unprotected blank cardstock represents the #1 vulnerability to the PIV System. Stolen cardstock enables very good counterfeits. Card production and issuance must provide for strict protections for blank cardstock – including personnel, physical, procedural, and audit security. This is particularly important at decentralized issuance sites.	Include strict protections for blank cardstock – including personnel, physical, procedural, and audit security This change has been included IAB Recommended Revisions to FIPS 201, Section 2.2.1.5.
78	IAB	Bob Donelson	G	D1.4.1.6.1	**FIPS 140-2 Level 3 Operator Authentication.** Achieving Level 3 requires that PINs not be passed to the card as plaintext. The PIN will have to be scrambled in some way – such as by encrypting or hashing. This is not what GSC-IS specifies, few if any of the cards and infrastructure deployed today support this. Implementing the change, especially if providing a smooth transition period, will be expensive – likely running into $10Ms or more. Unfortunately, this change gains at best a minuscule upgrade in security. The reason is that the card can only exert control over itself, it has no control over the environment is communicating with (which must be treated as untrusted). Scrambling the PIN will provide assurance that it cannot be captured and exploited by a rogue program running on the card. But the card is already pretty well locked down, and in some cases may be totally locked down.	Delete the requirement for FIPS 140-2 Level 3 Operator Assurance. It should be an option for achieving higher security levels, but not be required in the near term. This change has been incorporated in IAB Recommended Revisions to FIPS 201. The requirement which would naturally occur in Section 4 Has been deleted.
79	IAB	Bob Donelson	G	D1.4.1.4 D1.4.1.5 D1.4.2 D1.4.3 D1.4.4	**Required & Optional Elements.** With the 201 PD, it is difficult to determine what data, cryptographic, and biometric elements are required and optional on the various media of the PIV card. This is because this information is spread across the document and incompletely addressed.	FIPS 201 Should explicitly define data, cryptographic, and biometric elements that are minimum and mandatory by media type: • Graphical • Contact ICC • Contactless ICC • Magnetic Stripe • Bar Code For clarity and concision, these should be presented in a table. Implementation details and all optional elements for PIV credential data must be specified by media type in the PDMF of SP 800-73. This change has been incorporated in IAB Recommended Revisions to FIPS 201, Section 3.3

Cmt #	Org	Point of Contact	Type (G, E, T)	Section,Annex,etc and Page Nbr	Comment(Include rationale for comment)	Proposed change
80	IAB	Bob Donelson	G	D1.4.3, p 27, 28-29	**Restrictions on PIV Authentication Key.** From D1.4.3, the PIV Auth Key is "only available through the contact interface of the PIV card." The next sentence suggests [but fall short of explicitly stating] that PIV Auth private key operations are privileged and require activation. This is an area where 201 should allow issuers flexibility. Several departments and agencies represented in the IAB have strong requirements for physical access control. In many cases, these departments and agencies have determined that Physical access will largely occur without PIN entry. Furthermore, they wish to have the option of using the capabilities of the PIV card authenticate itself to the card reader using either the contact or contactless interface.	Clearly classify PIV Authentication Private Key operations to be non-privileged operations, so that cardholder or CMS activation is not required. All cryptographic operations are allowed across all interfaces as specified in SP 800-73 according to cross-agency interoperable use case requirements. This has been removed from the IAB Recommended Revisions to FIPS 201 and relegated to SP 800-73.
81	IAB	Bob Donelson	G	D1.4.4	**Restriction on Biometrics.** "The biometric data on the PIV card may only be read from an activated card through the contact interface." This is another area where 201 should allow issuers flexibility. Several departments and agencies represented in the IAB have identified strong requirements for physical access control with biometrics stored on the card used in locations where there is no PIN pad. Other departments and agencies require that biometrics be protected by PIN code and may never be transmitted across the contactless interface. 201 should accommodate both.	Delete "The biometric data on the PIV card may only be read from an activated card through the contact interface." Allow the issuer to determine which interfaces (contact, contactless, or both) the biometric may be read through and whether transmission of the biometric is a privileged operation requiring card activation. This issuer should document their determination together with the considerations and documenting the functional, usability, security, integrity, and privacy requirements. This has been removed from the IAB Recommended Revisions to FIPS 201 and relegated to SP 800-73.
82	IAB	Bob Donelson	G	Not Present	**Chain of Trust.** The chain of trust binding the cardholder, the issuer, the identity verification, the card and the biometric is not adequately presented.	Added to the IAB Recommended Revisions to FIPS 201, in Sections 2,2, 2.2.1, 2.2.1.4, and 7.2

December 21, 2004

To: National Institute of Standards and Technology
From: Interagency Advisory Board
RE: Federal Information Processing Standard 201 Rewrite

Attached, please find the collective submission of all agencies served by the Government Smart Card Inter-Agency Advisory Board (IAB). The IAB, in performing its task in accordance with the Terms of Reference between National Institute of Standards and Technology (NIST) and the IAB with respect to authoring of the NIST Special Publication (SP) 800-73, identified several issues directly impacting the SP800-73 in the November 8, 2004 Public Draft FIPS 201.

This effort represents a significant re-write of the public draft Federal Information Processing Standard (FIPS) 201. The resulting document re-organizes responsibilities, roles and systemic architecture to more accurately align with industry best practices, government processes for large scale credentialing and access control solutions. Key areas are:

- Separation of ID verification, validation and credential issuance from all other parts of the system:
  - Definition that ID Verification and Validation is in scope;
  - Established chain of trust for ID;
  - Removed technical specifications for card management;
  - Definition that trustworthiness for particular job/role is out of scope.
- Enhanced definition of the PIV credential's role in inter-agency interoperability by providing validated use case scenarios.
- Removed technical and informative discussion on Physical Access Control Systems and Logical Access Control Systems. The IAB resolved this information should be supported by OMB through technical implementation guidance and policy with a phased implementation plan.
- Clarification of role for SP800-73 to support the PIV application on the ICC. Enhanced this specification to provide complete definition of the PIV application, technical specifications and reference to existing NIST approved standards for compliance.

These changes represent a substantive impact on the original draft of the FIPS 201. The IAB offers to support NIST in understanding these changes. The IAB recommends NIST hold a discovery and rationale session to seek information from all parties submitting comments. The IAB will fully support this session at NIST's earliest convenience.

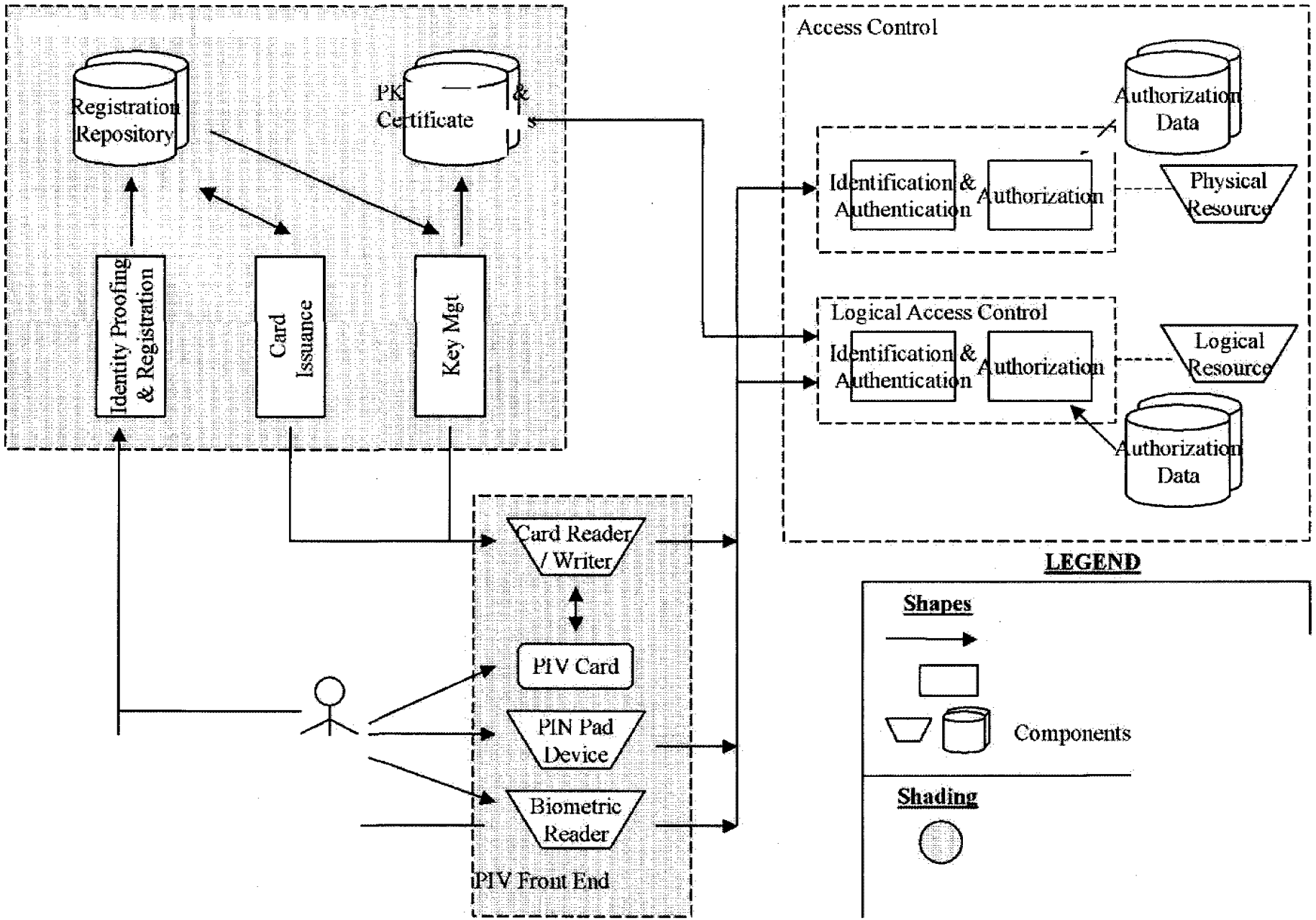
Enclosures:
2004-12-21 IAB FIPS 201 comments submission.xls – IAB Formal comments submission in the NIST required spreadsheet format
2004-12-21 IAB FIPS 201_Version 2_Final.doc – IAB Recommended revisions to FIPS 201
2004-12-21 IAB FIPS 201 Summary Changes.ppt – IAB Presentation summarizing the major elements of change in powerpoint presentation form

Enclosure(s):
Interagency Board Summary of Comments
IAB Recommended Changes to PIV

Enclosure(s):
Interagency Board Summary of Comments
IAB Recommended Changes to PIV

Summary of Changes

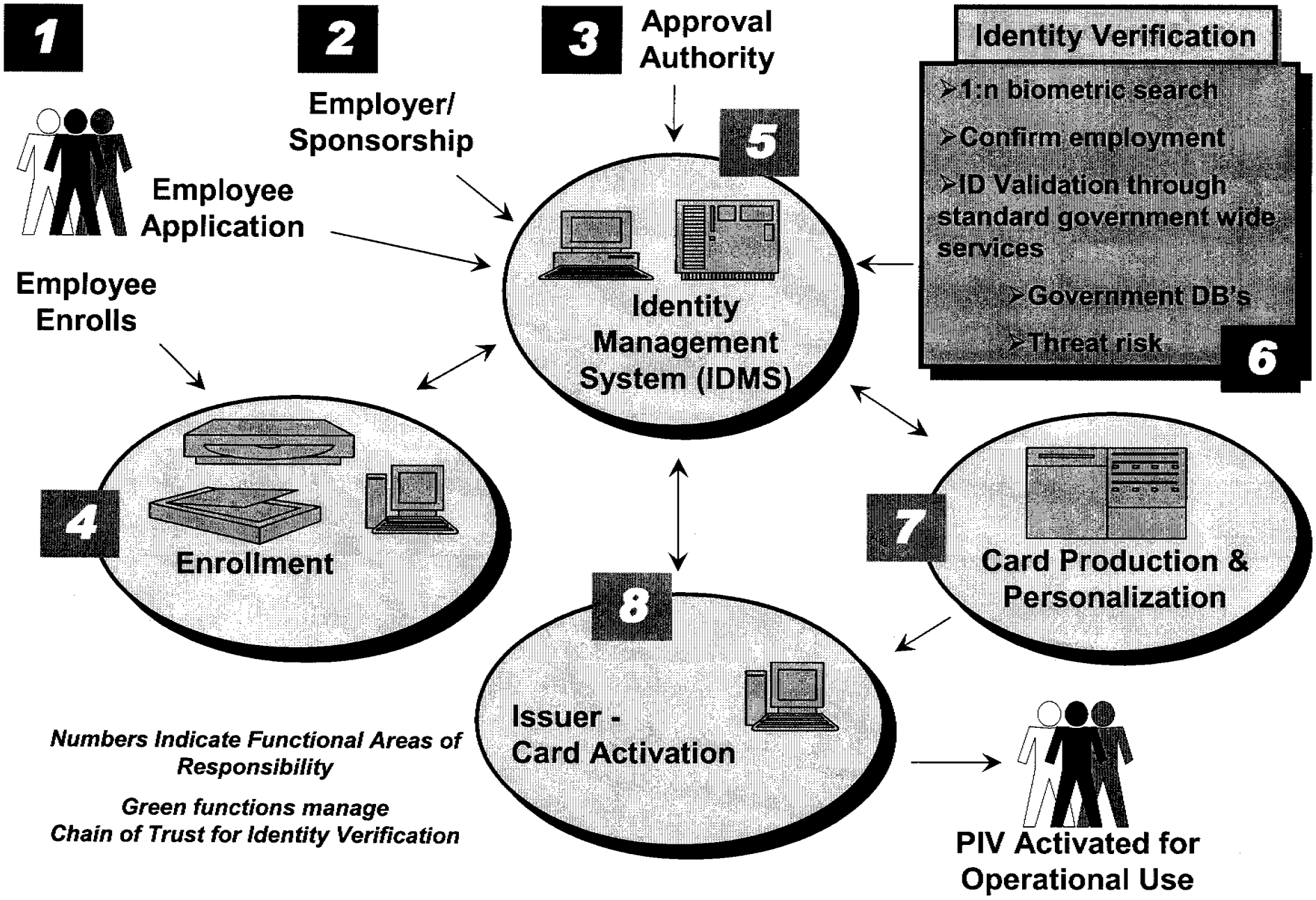
Core structural changes and rationale


Registration Repository
PK Certificate &
Identity Proofing & Registration
Card Issuance
Key Mgt
Access Control
Authorization Data
Identification & Authentication
Authorization
Physical Resource
Logical Access Control
Identification & Authentication
Authorization
Logical Resource
Authorization Data
Card Reader / Writer
PIV Card
PIN Pad Device
Biometric Reader
PIV Front End
LEGEND
Shapes
Components
Shading

Original FIPS 201

- Specified four major activities and systemic components in one flow
  - ID Verification and Validation
  - Credential issuance (Card management)
  - Logical access control systems (PKI management)
  - Physical access control systems (CHUID and Biometrics)
- Did not enable clean guidance for technical solutions and procurement

PIV Identity Verification and Issuance



Proposed FIPS 201

- Focuses intently on the Identity Management issue for HSPD-12 compliance
  - Strong chain of trust for credentialing using electronic processes
  - Identity verification and validation, not trustworthiness
  - Clean separation between ID management and card management
  - Future proofs the solution by placing technology specific issues within SP800-73 (e.g., cryptographic and biometric issues)
- Operational use is specified in use case scenarios
  - Clarifies inter-agency interoperability requirements
- Enables flexibility in procurement of all systemic components
  - IDMS
  - ID validation and verification solution
  - Card production/issuance
  - Enrollment
  - Logical solutions (PKI)
  - Physical access control solutions

IAB RECOMMENDED REVISIONS TO FIPS 201

21 December 2004

Version 2.0

TABLE OF CONTENTS

1 Introduction

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

A wide range of mechanisms are employed to authenticate identity, leveraging many different classes of identification identity credentials. For physical access, individual identity has traditionally been authenticated by use of paper credentials, such as driver's licenses and badges. Logical access has traditionally been authenticated through user-selected passwords. More recently, cryptographic mechanisms and biometric techniques have been applied to physical and logical security, replacing or supplementing the traditional credentials.

The strength of the authentication that is achieved varies, depending upon the type of credential, the process used to issue the credential, and the authentication mechanism used to validate the credential and the bearer of the credential. This document establishes a standard for personal identity verification based on secure and reliable forms of identification credentials issued by the Federal Government to its employees and contractors. These credentials are intended to authenticate individuals that require access to Federally-controlled facilities, information systems, and applications.

This standard addresses requirements for identity proofing, infrastructures to support interoperability of identity credentials, and validation and accreditation of applications and processes. This standard provides technical mechanisms to support authentication of the bearer and the credential to physical and logical access systems. This standard does not specify physical and logical access control mechanisms and processes.

1.1 Purpose

The purpose of this standard is to specify a reliable cross-agency interoperable Personal Identity Verification (PIV) system for use in applications such as access to Federally-controlled facilities and information systems. This standard has been developed within the context and constraints of Federal policy and information processing technology currently available and evolving.

This standard defines requirements for a PIV system within which common identification credentials can be established and shared.

Homeland Security Presidential Directive 12 (HSPD-12), signed by the President on August 27 2004, established the requirements for a common identification standard for identification issued by Federal departments and agencies to Federal employees and contractors (including contractor employees) for gaining physical access to Federally-controlled facilities and logical access to Federally-controlled information system as defined by the interoperable use cases in SP800-73. HSPD-12 directs the Department of Commerce to develop a Federal Information Processing Standard (FIPS) to define such common identification credential. In accordance with the HSPD-12, this standard defines the minimum mandatory technical requirements for the identity credential that is:

- Issued based on sound criteria for verifying an individual's identity;
- Resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation;

- Rapidly authenticated electronically;
- Issued only by providers whose reliability has been established by an official accreditation process; and
- Recognized by and interoperable with all federal departments.

The standard stipulates identification validation verification requirements and graduated authentication/security mechanisms for PIVs offering varying degrees of security in operational use. Note that the Federal departments and agencies must determine the authentication mechanisms appropriate for their applications. Therefore, the scope of this standard is limited to authentication of an individual's identity.

Out of scope matters include:

- Access authorization decisions;
- Back end systems required for transmission and processing of authentication and validation; and
- All federal data and processes not related to authentication as specified herein.

1.2 Document Organization

This standard is composed of two parts, PIV-I and PIV-II. The first part (PIV-I) describes the minimum requirements for a Federal personal identification verification and issuance system that meets the control and security objectives of the HSPD-12, including the personal identity proofing process for federal employees but does not address the interoperability of PIV cards and systems among agencies. The second part (PIV-II) provides PIV card, cryptographic, biometric, and card reader specifications necessary for achieving cross-agency operation. PIV-II fulfills the HSPD-12 mandate for graduated criteria from least to most secure.

Implementers of the standard should note that this document is normative. This standard does not restrict the agencies from adopting additional alternatives.

Technical specifications of the FIPS 201 credential are published in an addendum document Special Publication (SP) 800-73.

PART 1: PIV-I

This part describes the minimum requirements for a Federal personal identification system that meets the control and security objectives of the HSPD-12, including the personal identity proofing process.

Implementation Timeframe: In accordance with HSPD-12, agencies shall meet the requirements of this part no later than October 2005, in accordance with OMB phased implementation guidance.

2 Common Identification and Security Requirements

This section provides the requirements for the first part of the PIV standard. PIV-I addresses the fundamental control and security objectives outlined in HSPD-12, including the personal identity proofing process for new employees and contractors. Note that PIV-I does not address interoperability of PIV cards and systems among agencies or compel the use of a single, universal credential. However, in accordance with HSPD-12, Federal agencies using smart cards should be PIV-I compliant no later than October, 2005.

PIV-II describes the policies and minimum requirements of a PIV card that allows interoperability of credentials for physical access and logical access.

The technical requirements for implementing PIV policies are described in detail in NIST SP 800-73 and associated guides.

2.1 Control and Functional Objectives

HSPD-12 established control objectives for secure and reliable identification of Federal employees and contractors. These control objectives, provided in paragraph 3 of the directive, are quoted here:

> (3) "Secure and reliable forms of identification" for purposes of this directive means identification that (a) is issued based on sound criteria for verifying an individual employee's identity; (b) is strongly resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation; (c) can be rapidly authenticated electronically; and (d) is issued only by providers whose reliability has been established by an official accreditation process. 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).

Each agency's PIV implementation shall meet the four control objectives listed above. The agency PIV systems shall have six functional objectives:

1. Use an identity proofing and enrollment process;
2. Use a secure identity credential issuance process;
3. Issue interoperable credentials through systems and providers whose reliability has been established by the agency and so documented and approved in writing;
4. Issue identity credentials that are resistant to fraud, tampering, counterfeiting, and terrorist exploitation;
5. Implement an identity credentialing system that supports rapid electronic authentication of Federal employees and contractors government-wide during operational use for access control decisions; and
6. Support credentials for physical and logical access to Federally controlled facilities and information systems government-wide.

This common PIV card supports the control objectives listed above and, with the Government-wide interoperable credential issuance process and issuer Certification and Accreditation already established in PIV-I, allows agencies to both trust and use the PIV credentials of other agencies for physical and logical access control.

2.1.1 PIV Use Cases and Requirements

The PIV is a secure inter-department identity credential. The essence of credential interoperability is the ability to authenticate credentials before granting physical or logical access. Detailed use cases and requirements to achieve inter-agency interoperability shall be specified in SP800-73.

2.1.2 Definitions

Identity Proofing – Validation of claimed identity of individual.

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

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

Authentication – The secure checking of a credential against its issuer.

Credential – A token (digital or printed) that represents the relationship between the bearer and the issuer.

PIV Credential – A secure credential that binds the issuer to the credential to the biometric to the identity validation.

Applicant – Employee/Contractor requiring unescorted access to physical facilities and access to logical systems and/or networks.

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

2.1.3 Scope of PIV-I

To meet the control objectives for secure and reliable identification specified in HSPD-12, PIV-I shall:

- Provide identity proofing;
- Provide identity binding; and
- Enable identity authentication of the individual using a PIV credential supporting reliable and effective trustworthiness decision processes.

2.2 Identity Proofing and Enrollment Process

For compliance to the PIV-I control objectives in Sections 2.1, at a minimum, agencies shall follow the identity proofing and registration process defined in Sections 2.2.1- 2.2.4 when issuing identity credentials. *Figure 1- PIV Identity Verification and Issuance* shows the logical components that comprise a PIV identity proofing and credentialing process. This diagram illustrates the minimum mandatory components and roles required to support PIV I.

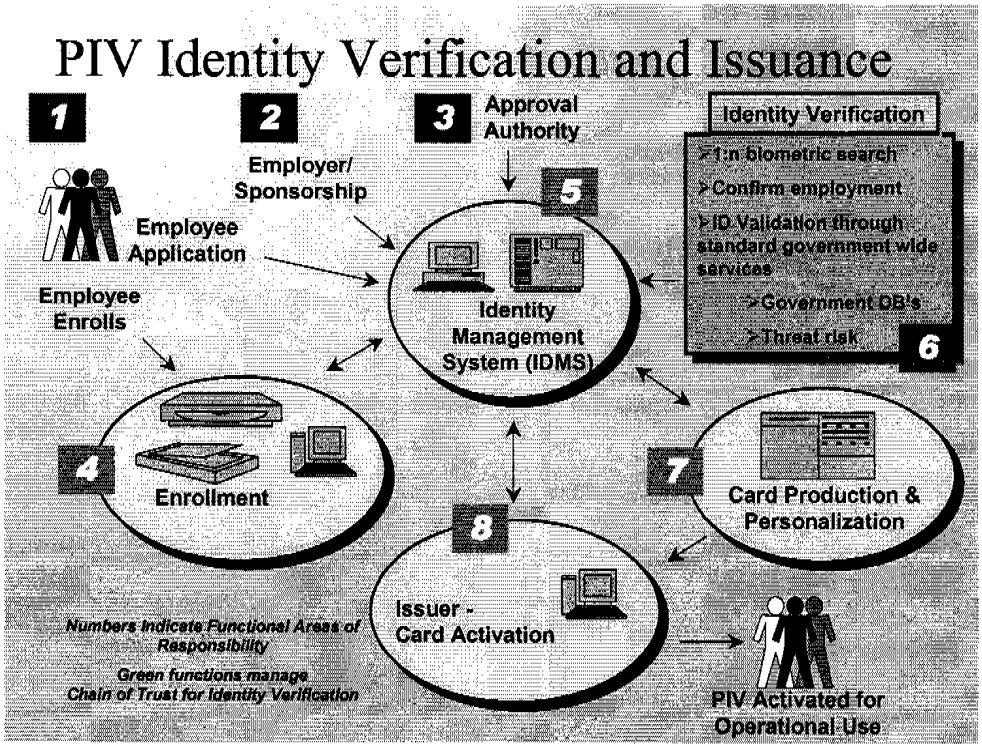


Figure 1- PIV Identity Verification and Issuance

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

- Applicant – The individual to whom an identity credential is to be issued. Individual shall provide supporting enrollment documentation for claimed identity.
- Employer/Sponsor – Shall substantiate the relationship to the Applicant and provide sponsorship of Applicant. Shall authorize the request for a PIV credential.
- Approval Authority – Shall establish organizational chain of command within the IDMS for PIV application approvals. This includes establishing approved Employer/Sponsors. May designate automated or manual approval processes for completed PIV applications. Shall manage the total scope of the chain of trust established in functional process. Shall manage appropriate privacy and security controls.
- Issuing Authority (Issuer) – The entity that issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The issuer shall complete the chain of trust by performing 1:1 biometric check of the applicant against the PIV enrollment record. Upon confirmation of correct individual, the issuer shall activate the card. The issuer shall then release the credential to the individual.

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

The Approval Authority shall practice best practices for separation of roles and responsibilities according to risk. The Approval Authority shall ensure the system has at least two persons performing different functions in the chain of trust processes.

The roles of Enrollment and Issuer may be the same individual and the same physical facility. Card production may be done either centrally or at a distributed issuer facility, provided security and quality control objectives for card stock management are fully met. The Applicant must appear for at least one face to face encounter before the issuance of a PIV card.

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

- Identity Management System (IDMS) – The Approval Authority shall maintain the ID Management System that shall be the system of records for PIV credentials issued. It performs the identity proofing, verification and validation to establish identity claim validity. Shall provide a 1:many search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services (6) which shall be provided in accordance with HSPD-11. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.
- Enrollment System– Initiates the chain of trust for identity proofing. Enrollment shall provided trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.
- Card Production and Personalization System– Shall provide full inventory controlled process to print and personalize PIV credentials per approval of the IDMS. Shall provide mechanisms to track status, control inventory, and protect blank card stock and personalized/printed card stock prior to activation.

PIV Identity Proofing and Issuance Requirements and Workflow are:

- Applicant – The individual to whom an identity credential is to be issued. Individual shall provide supporting enrollment documentation for claimed identity.
- Employers/Sponsors – Shall substantiate the relationship to the Applicant and provide sponsorship of Applicant. Shall authorize the request for a PIV credential.
- Approval Authority – Is responsible for and shall manage the total scope of the chain of trust established in functional process areas 4 through 8 in *Figure 1*.
- Enrollment – Initiates the chain of trust for identity proofing. Enrollment shall provided trusted services to confirm employer sponsorship, bind the Applicant to their biometric, and validate identity claim documentation. Enrollment delivers a secured enrollment package to the IDMS for adjudication.
- IDMS (Identity Management System) – The Approval Authority shall maintain an IDMS that shall be the system of records for PIV credentials issued by that Approval Authority. The IDMS performs the identity proofing, verification and validation to establish identity claim

validity. Shall provide a search to ensure the applicant has not enrolled under a different name. Shall confirm employment appropriate to the PIV request. Shall manage identity validation and verification services through government-wide standardized services (6) which shall be provided in accordance with HSPD-11. Shall manage adjudication of identity claim. Shall approve issuance of PIV to applicant upon successful adjudication of identity claim.

- Card Production and Personalization – Shall provide full inventory controlled process to print and personalize PIV credentials per approval of the IDMS. Shall provide mechanisms to protect blank card stock, consumable supplies, and personalized/printed card stock prior to activation.
- Issuer – The entity that issues the identity credential to the Applicant after all identity proofing, background checks, and related approvals have been completed. The issuer shall complete the chain of trust by: performing 1:1 biometric check of applicant against PIV enrollment record, verifying photograph in enrollment record matches the individual. Upon confirmation of correct individual, the issuer shall activate the card. Upon activation, the issuer shall close the chain of trust by having the individual verify their biometrics against the PIV credential. The issuer shall then release the credential to the individual.

2.2.1 Identity Proofing and Enrollment

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

2.2.1.1 Employer/Sponsor

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

2.2.1.2 PIV Application Process

The PIV Application Process has four components:

1. The Applicant request and claimed identity documentation,
2. The employer/sponsor approval of Applicant request,
3. The approval authority confirms and approves PIV application, appropriate sponsorship, and shall approve the PIV request,
4. The enrollment to bind the submissions from (1), (2) and (3) for formal submission to the IDMS initiating the identity verification and validation process.

The Applicant shall provide a formal request for a PIV.

The Employer/Sponsor shall approve the Applicant request.

Once the Applicant has gained the sponsorship and approval of the Employer, the Applicant shall appear for Enrollment. The Applicant shall provide a minimum of two forms of identification from the list of acceptable documents included in the *Form 1-9, OMB No. 1115-*

0136, Employment Eligibility Verification to the PIV Registration Authority. At least one of the documents shall be a valid State or Federal Government-issued picture ID.

2.2.1.3 PIV Enrollment Process

The PIV Enrollment process shall provide the following minimum steps:

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

The PIV Binding process shall provide the following minimum steps:

6. Enrollment shall take biometric samples and photograph of the Applicant;
7. Enrollment shall manage the quality assurance process of the biometric and photographic capture. The biometric samples shall be verified to ensure proper performance; and
8. Enrollment shall bind the completed electronic enrollment package with a digital signature and forward the enrollment application to the IDMS for identity verification and validation.

The completed PIV enrollment package shall include:

- Scanned documents supporting identity claim;
- Biometric samples and digital photograph;
- Personal biographic and organizational information; and
- Digital signature of Enrollment Official.

2.2.1.4 Identity Verification Process

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

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

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

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

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

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

The IDMS shall be responsible to maintain:

- Completed and signed PIV enrollment package;

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

The IDMS shall provide services that:

- Notify the Employee/Contractor Applicant of status of the PIV;
- Notify the Employer of status of the PIV; and
- Enable validation by anyone inquiring if an issued credential is still valid.

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

2.2.1.5 Card Production, Activation and Issuance

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

Card production services shall:

- Maintain full inventory control of blank initialized or pre-issued (e.g. with the manufacturers keys) stock, consumables and manufacturing materials;
- Maintain a list of approved IDMS systems that can submit PIV requests for card production,
- Provide acknowledgement of IDMS request to produce a PIV;
- Notify the IDMS upon completion of PIV credential production;
- Maintain a list of approved Issuers that can activate and issue PIV credentials;
- Only send information regarding production of PIV credentials to approved authorities;
- Only send fully completed and personalized PIV credentials to approved Issuing Agents; and
- Document, implement, and maintain a Card Production, Activation and Issuance Security Policy.

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

2.2.1.6 Suspension, Revocation and Destruction

It is important to keep track of active cards as well as lost, stolen and expired cards. The guidelines for using some form of card registry will be covered in SP 800-73 and companion documents.

2.2.2 Re-issuance to Current PIV Credential Holders

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

- Insure the IDMS record for this individual states the credential is not expired;
- Verify the individual with a 1:1 biometric match against the IDMS record;
- Verify the individual against the IDMS record digital photograph;
- Recapture biometrics;
- Issue a new credential and update the IDMS record; and
- The recaptured biometrics and new credential record shall be digitally signed by the Issuing Authority.

2.2.3 Access Pending Identity Proofing

Until the required ID verification, validation and 1:many search is completed, new employees and contractors shall not be issued PIV credentials but shall be handled according to established visitor procedures.

2.2.4 Identity Proofing and Enrollment of Overseas Foreign Workers

Citizens of foreign countries who are working for the U.S. Federal Government overseas shall comply with all procedures and practices outlined in this standard. The U.S. Department of State Bureau of Diplomatic Security shall determine ID verification and validation processes for country specific requirements.

PART 2: PIV-II

This part provides detailed proposed operational and functional requirements for interoperability of PIV cards with the personal authentication, access control, and PIV card management systems across the Federal Government.

Implementation Timeframe: OMB has advised NIST that it plans to issue guidance regarding agency development of transition plans to Part 2.

3 PIV Card Specifications

3.1 Physical Specifications

1. PIV card physical characteristics shall comply with the following established standards:
   - ISO/IEC 7810
   - ISO/IEC 10373
   - ISO/IEC 7816
   - ISO/IEC 14443
2. The card shall contain a contact ICC interface;
3. The card shall contain a contactless ICC interface;
4. May be implemented with one or more ICCs; and
5. The card shall not be embossed, punched, or affixed with decals.

3.2 Physical Security Tamper Proofing and Resistance

6. The PIV card shall include the minimal set of standard PIV physical security devices for card stock, printed features, laminates and the ICC.
7. The PIV card may include additional standard PIV physical security devices.
8. These shall be specified in SP 800-73 and additional restricted documents.

3.3 PIV Credential Data

9. This section presents the key elements for the PIV data model:
10. Graphical data (Front and Back of card)
11. ICC data (Contact and Contactless)
12. Machine readable data (Barcode and magnetic stripe)
13. All information printed and stored on a PIV credential shall conform to the Pluggable Data Model Framework (PDMF) as specified in the SP 800-73. The PDMF provides minimum mandatory fields and the extension framework required for issuer specific options.
14. The following table enumerates by media type, what information is *required* and what is *optional*:

Media	Required	Optional
Graphical	• Photo • Name • Affiliation • Expiration Date • Agency CSN (GUID) • Mandatory Security Features	• Signature • Pay Grade • Rank • Bar Code • Agency Name • Agency Seal • Emergency Responder Info • Emergency Responder Language • Person ID • Issue Date • Return To • Physical Characteristics • Title 18 Language • Lost Card Info • Issuer ID • Color Coding (shall not interfere

		with mandatory security features) • Optional Security Features
Graphical: DOD Geneva Convention Data	• Medical • Date of Birth • SSN	
Contact ICC	• PIN • CHUID • PIV Auth Key • 2 Fingerprints • Facial image • All text data printed on card surface	• Remaining IAB PDMF • Digital Signature Key & Cert • Digital Signature PIN • Key Management Key • Card Management Key • Local Auth Key • Cyber ID Key and Cert • Emergency Responder Data
Contactless ICC	• PIN • CHUID • PIV Auth Key • 2 Fingerprints • All text data printed on card surface	• Remaining IAB PDMF • Key Management Key • Card Management Key • Local Auth Key • Facial image • Emergency Responder Data
Magnetic Stripe	None	FASC-N
Bar Codes	None	?

3.4 Graphical Data

15. The PIV card shall conform to a common format on the front of the card, and one of two common formats for the reverse.
16. All optional fields are under the control and discretion of the issuer. If an optional field is used as defined it shall be in accord with this standard. Per the issuer's discretion, optional zone areas may be used for other purposes.
17. The zones are enumerated below:

Note that the location (horizontal and vertical offsets) and size (width and height) remain to be completely specified in FIPS 201. These are TBD. Add pictures

Zn	Opt/ Req	Field	H-off	V-off	W "	Ht "	Description
f1	Req	Photo			1.08	1.45	Full frontal, top of head to shoulder, 300 dpi
f2	Req	Name					Arial Bold, all caps, ≥10 pt Surname above, first name below
f3	O	Signature					
f4	O	Pay Grade					Format at discretion of Issuer
f5	O	Rank					Format at discretion of Issuer
f6	O	Bar Code					PDF417
f7	Req	Contact I/F					
f8	Req	Affiliation					Arial Bold Black, all caps, ≥7 pt
f9	Req	US Government					Arial Bold Black, all caps, ≥7 pt
f10	O	Agency Name					Arial Black. ≥7 pt
f11	O	Agency Seal					Arial Black. ≥7 pt (?)
f12	O	Emergency Response					Font ???. Size ??? "Federal Emergency Response Official"
f13	O	Issue Date					"Expires", Arial Black, ≥6 pt, "YYYY/MM", Arial Black, ≥10 pt
f14	Req	Expiration Date					"Expires", Arial Black, ≥6 pt, "YYYY/MM", Arial Black, ≥10 pt

Zn	Opt/ Req	Field	H-off	V-off	W "	Ht "	Description
r1	O	Agency CSN (GUID)					Arial Bold, ≥10 pt, Format at discretion of Issuer
r2	O	Issuer Id Number					Arial Bold, ≥10 pt, Department Code (6 characters) + Agency Code (4 characters) + Issuing Agency (5 digits)
r3	O	Magnetic Stripe					Hi-Co. Placement per ISO/IEC 7811
r4	O	Return To					Return Address - Arial. ≥6 pt
r5	O	Physical Characteristics					Arial Black. ≥7 pt e.g. height, eye color, hair color
r6	O	ER Language					Arial. ≥5 pt "The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas."
r7	O	Title 18 Lang.					Arial. ≥6 pt
r8	O	Lost Card					Instructions - Arial. ≥6 pt
r9	O	3 of 9 Bar Code					iaw AIM standards

Zn	Opt/ Req	Field	H-off	V-off	W "	Ht "	Description
m1		Magnetic Stripe					
m2		Medical					
m3		Date of Birth					
m4		SSN					
m5		Bar Code					
m6		Control Number					
m7		Date					
m8		Property USG					
m9		Geneva Conv C					

Samples of Printed Fields

Zn	Field	Sample
f2	Name	SURNAME FIRSTNAME
f8	Affiliation	**CONTRACTOR**
f9	US Government	**UNITED STATES GOVERNMENT**
f14	Expiration Date	**Expires** **2008/06**
r1	Agency CSN	**USANIST0101842**
r2	Issuer Id Number	**USADOCNIST00001**
f4	Pay Grade	*Unspecified*
f5	Rank	*Unspecified*
f10	Agency Name	**US Agency**
f11	Agency Seal	*This is a picture, not print*
f12	Emergency Response	*Unspecified*
f13	Issue Date	**Issued** **2008/06**
r4	Return To	Return to: Security Manager's Office (CAPS) 1800 F Street, N.W. Washington, DC 20405
r5	Physical Characteristics	**Height** **5'11"** **Eyes:** **Brown** **Hair:** **Brown**
r6	ER Language	The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas.
r7	Title 18 Lang.	This credential is the property of the United States Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.
r8	Lost Card	Drop in any post office box for return.

3.5 ICC Data

18. The PIV card shall include the minimum mandatory data electrically in an ICC on the credential as specified in the PDMF, as specified in SP 800-73.

4 Cryptographic Specifications

19. The PIV card must support at least one public/private key pair. A certificate for the minimum mandatory public/private key is optional.
20. The PIV card must perform all private key cryptographic operations on card.
21. The PIV card must support key pair generation.
22. The PIV is not required to support public key operations (e.g., verify).
23. The PIV card must support key injection under Issuer control.
24. The PIV card must support importation and storage of X.509 certificates.
25. Cryptographic algorithms are specified in FIPS 186-2 (Digital Signature Standard), FIPS 197 (Advanced Encryption Standard) and FIPS 46-3 (Data Encryption Standard).

26. All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.
27. All PIV cryptographic keys shall be stored within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.

28. The PDMF shall use OIDs throughout all cryptographic specifications binding the algorithm, parameters, and key length.
29. PIV credential relying parties shall use these OIDs to enable in protocol definitions to provide future proofing protection against unknown and unforeseen attacks on any given cryptosystem.
30. Use of ECC shall comply with NIST approved curve definitions and parameters. Issuers shall not be allowed to self select curves and parameters.

5 Biometric Specifications

31. Biometric data shall be collected and used as follows:
    - Ten fingerprints, to support law enforcement check during the application process;
    - Two fingerprint templates shall be extracted from the ten "slap" fingerprints to be stored on the card for automated verification process. The two fingerprints are also allowed to be taken separately electronically, instead of being extracted from the ten "slap" fingerprints; and
    - An electronic facial image, to be stored on the card for alternate identity verification.
32. Biometric data should be used in One to Many checking to support duplicate identities within a single Department or agency.
33. Biometric data on a PIV card may be read through the contact or contactless interface. Access control management for biometrics shall be specified in SP800-73 per the PDMF and the phased implementation plan.
34. The format for the storage and exchange of the biometric information captured and used in the PIV system shall conform to NIST approved ANSI standards. These standards shall be as specified in SP800-73.

5.1 Fingerprint Biometric

35. Fingerprints shall be the primary biometric used in the PIV system.
36. Exemptions for foreign nationals may be made due to international law.
37. Fingerprint preference, in decreasing order, is: index, middle, ring and thumb. Little fingers shall not be used.
38. The two fingerprints should not be from the same hand if possible.

5.2 Facial Biometric

39. Facial images are captured:
    - When fingerprints are unavailable
    - Multimodal applications that require face as well as fingerprint to lower FAR
    - Visual inspection
40. There is no mandatory requirement for algorithmic facial recognition systems should fingerprint not be available.

5.3 PIV Registration [Biometric Enrollment] and Issuance

41. When applicants are unable to present fingerprints, e.g. due to disability, the facial image is sufficient.
42. Biometric data (2 fingerprints and 1 face) shall be embedded in the PIV card during personalization

43. All biometric data on the PIV card shall be digitally signed by the IA

Biometric data quality, format, integrity and confidentiality will be described in SP 800-73.

6 Card Reader Specifications

SP800-73 specifies minimum cross-agency interoperable transaction requirements and a phased implementation plan. Card Reader Specifications will be developed to support procurement practices that enable these transactions and phased plans. These specifications shall provide appropriate protection of keying material, PINS and biometric data.

The following are known minimum mandatory specifications that shall be supported.

6.1 Contact Reader Specifications

44. Contact readers shall conform to ISO/IEC 7816 for card-to-reader interface.
45. Contact readers shall conform to PC/SC for reader-to-host system interface in those cases where they are connected to general purpose desktop computing systems.

6.2 Contactless Reader Specifications

46. Contactless readers shall conform to ISO/IEC 14443 for card-to-reader interface.
47. Contactless readers shall conform to PC/SC for reader-to-host system interface in those cases where they are connected to general purpose desktop computing systems.

7 Graduated Criteria

HSPD-12 mandates formulation of a Federal standard for "*Secure and reliable forms of identification,*" and defines this to mean:

(a) is issued 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;
(d) is issued only by providers whose reliability has been established by an official accreditation process.

Graduated criteria are provided for (b) and (c) in the following sections.
Security levels for graduated criteria shall be determined by implementation guidance. The following provides guidance for selection of graduated criteria.

7.1 Resistance to Tampering & Counterfeiting

7.1.1 Graphical Resistance to Tampering & Counterfeiting

	Criteria	Description
GR1	Similar Appearance	Departments & agencies are free to follow general guidelines, so that all PIVs have about the same graphical elements in about the same place using about the same fonts and sizes (E.g FIPS 201 PUBLIC Draft section 4.1.4)
GR2	Uniform Appearance	PIVs adhere to a tight standard for graphical appearance, including a clear specification of: • Background color & pattern • Zone location to within a tight tolerance (.01 inch) • Font sizes (eliminate "minimum" where possible) • Additional printing (what is allowed & where)
GR3	+ Security Feature	Uniform Appearance + All PIVs have a uniform and recognizable security feature (e.g. Holographic overlay, OVI)
GR4	+ Multiple Security Features	Uniform Appearance + All PIVs have a uniform set of recognizable and testable security features. Possibilities include: • OVI • Holographic overlay • Guilloche • Very fine line • Micro printing • Laser engraving • Laser printing • UV inks • Hidden word • Digital watermarking • Laminate glues Final set of required security features is TBD. This list is closely held and shared with qualified manufacturers on a "need to know" basis.

7.1.2 Electrical Resistance to Tampering & Counterfeiting

These criteria shall be fully specified in SP800-73. The following are examples for consideration.

Note: these criteria are not mutually exclusive, they must be applied in combination		
Level	Criteria	Description
Medium	Level 2 Physical Security	The ICC module conforms to FIPS 140-2 Level 2 requirements for Physical Security
Medium	PIN Length	The ICC enforces a PIN length of 6 digits or longer
Medium	PIN Protection	The ICC enforces "READ NEVER" on Card PINs
Medium	Key Protection	The ICC enforces "READ NEVER" on Private and Secret Keys
High	Countermeasures	The ICC employs countermeasures against SPA and DPA attacks
High	Environment Sensors	The ICC employs sensors to detect attacks that vary environment ambient conditions (e.g. temperature, voltage) out of range
High	Level 3 Physical Security	The ICC module conforms to FIPS 140-2 Level 3 requirements for Physical Security

High	WRITE NEVER	The ICC enforces a "WRITE NEVER" across the entire card policy after issuance

7.2 Electronic Authentication

Establishing a chain of trust is a result of performing both a PIV Authentication and Cardholder Authentication. PIV cards contain the mechanisms to support any level of PIV and cardholder authentication. It is up to the PIV Infrastructure to use this information to establish the desired level of chain of trust.

Implementing Departments and Agencies have the flexibility to choose the authentication mechanisms that allow them to achieve the desired overall confidence in the chain of trust.

7.2.1 Cryptography

The PIV card has a single mandatory key and several types of optional keys as define below:

- The *PIV authentication* key is an asymmetric private key supporting logical and physical access and is mandatory for each PIV card;
- The *local authentication* key may be either a symmetric (secret) key or an asymmetric private key for physical access and is optional;
- The *digital signature key* is an asymmetric private key supporting document signing and is optional;
- The *key management key* is an asymmetric private key supporting key establishment and transport and is optional; and
- The *card management key* is a symmetric key used for personalization and post-issuance activities.
- Algorithms and key sizes for each PIV key type are specified in the following table:

Table 4-5: PIV Key Type

PIV Key Type	Time Period	Algorithms & Key Sizes
PIV authentication key	Through 12/31/2010	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Local authentication key	Through 12/31/2010	Two Key Triple-DES (TDEA2) Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256 RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher
	After 12/31/2010	Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256 RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Digital signature key	Through 12/31/2008	RSA/DSA 1024 bits or higher; ECDSA 160 bits or higher

	After 12/31/2008	RSA/DSA 2048 bits or higher; ECDSA 224 bits or higher
Key management key	Through 12/31/2008	RSA/D-H 1024 bits or higher; ECDH 160 bits or higher
	After 12/31/2008	RSA/D-H 2048 bits or higher; ECDH 224 bits or higher
Card management key	Through 12/31/2010	Two Key Triple-DES (TDEA2) Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256
	After 12/31/2010	Three Key Triple DES (TDEA3) AES-128, AES-192, and AES-256

7.2.2 PIV PKI Authentication

These will be vetted and expanded in accord with Policy group Use Cases for minimum mandatory interoperability.

	Level	Criteria	Description
	Low	Data Present	Data is read on PIV, no cryptographic checking of any kind
1	Medium	Data Present	Issuer-signed data is found on the PIV and verified
2	Medium	+ PIV Challenge	Above + PIV demonstrates it knows the authentication secret (e.g. it signs a random challenge with the PIV Authentication private key, which the reader then verifies with the public key)
3	Medium	+ Cert Check	Above + Reader verifies authenticity of PIV Auth Cert (by verifying the issuers digital signature)
4	Medium	+ Expired Check	Above + Reader checks the expiration date in the certificate
5	High	+ CRL Check	Above + Reader checks most recent CRL from issuer to verify certificate has not been revoked
6	Ultra High	+ Issuer Check	Above + Reader performs a real time check with issuer service to verify that certificate is still valid

7.2.3 Cardholder Authentication

These will be vetted and expanded in accord with Policy group Use Cases for minimum mandatory interoperability.

	Level	Criteria	Description
1	Low	Possession	Cardholder is in possession of the card
2	Medium	Card + PIN	The cardholder has successfully entered the PIN
3	High	Card + Bio	The cardholder has successfully passed a biometric match
4	Ultra High	Card + PIN + Bio	The card holder has successfully entered the PIN and passed a biometric match.

Note: This scheme applies whether the authentication is performed by the card or by an external entity (reader, PC, door controller…) *The guiding principal is that the authenticating entity must perform the match.* Thus:

- Card-based: The card must perform the PIN validation and/or biometric match.
- External Auth: External entity must perform the PIN validation and/or biometric match.

7.2.4 PIV Card Authentication

These will be vetted and expanded in accord with Policy group Use Cases for minimum mandatory interoperability.

	Level	Criteria	Description
1	Low	Data Present	Issuer-signed data is found on the PIV
2	High	+ CRL Check	Above + Reader checks most recent CRL like interface from issuer to verify the card not been revoked
3	Ultra High	+ Issuer Check	Above + Reader performs a real time check with issuer service to verify that certificate is still valid

8 Identity Validation Transactions

8.1 Transaction Pair Description

The following describe the Identity Validation Transactions that a Registration System and a Issuer Validation system would need to have in common:

1. Registration: Pass the CHUID and ask is this a valid Card
   Validation Response: Yes or NO
2. Registration: Pass the X.509 Certificate (as an identifier) and ask is this a valid Card
   Validation Response: Yes or NO
3. Registration: Pass the CHUID and ask is this a valid Cardholder for Photo identification
   Validation Response: Returns a Picture
4. Registration: Pass the CHUID plus fingerprint and ask is this a valid Cardholder.
   Validation Response: Yes or NO
5. Registration: Pass the X.509 Certificate (as an identifier) and ask is this a valid Certificate.
   Validation Response: Yes or NO