Req#	Requirement	Source	Section Title
FIPS 201-1			
1.1-1	Credentials shall be issued only to individuals whose true identity has been verified.	FIPS 201, Section 2.1	Control Objectives
1.1-2	Credentials shall be issued only after a proper authority has authorized issuance of the credential.	FIPS 201, Section 2.1	Control Objectives
1.1-3	Only an individual with a background investigation on record shall be issued a credential.	FIPS 201, Section 2.1	Control Objectives
1.1-4	An individual shall be issued a credential only after presenting two identity source documents, at least one of which is a valid Federal or State government issued picture ID.	FIPS 201, Section 2.1	Control Objectives
1.1-5	Fraudulent identity source documents shall not be accepted as genuine and unaltered.	FIPS 201, Section 2.1	Control Objectives
1.1-6	A person suspected or known to the government as being a terrorist shall not be issued a credential.	FIPS 201, Section 2.1	Control Objectives
1.1-7	No substitution shall occur in the identity proofing process. More specifically, the individual who appears for identity proofing, and whose fingerprints are checked against databases, must be the person to whom the credential is issued.	FIPS 201, Section 2.1	Control Objectives
1.1-8	A credential shall not be issued unless it has been requested by proper authority.	FIPS 201, Section 2.1	Control Objectives
1.1-9	A credential shall remain serviceable only up to its expiration date. More precisely, a revocation process exists such that expired or invalidated credentials are swiftly revoked.	FIPS 201, Section 2.1	Control Objectives
1.1-10	A single corrupt official in the process shall not have the ability to issue a credential with an incorrect identity or to a person not entitled to the credential.	FIPS 201, Section 2.1	Control Objectives
1.1-11	An issued credential shall not be [easily] modified, duplicated, or forged	FIPS 201, Section 2.1	Control Objectives
1.1-12	The organization shall adopt and use an approved identity proofing and registration process.	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements
1.1-13	The process shall begin with initiation of a National Agency Check with Written Inquiries (NACI) or other Office of Personnel Management (OPM) or National Security community investigation required for Federal employment. This requirement may also be satisfied by locating and referencing a completed and successfully adjudicated NACI. At a minimum, the National Agency Check (NAC) shall be completed before credential issuance. Appendix C, Background Check Descriptions, provides further details on NAC and NACI.	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements
1.1-14	The applicant must appear in-person at least once before the issuance of a PIV credential.	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements
1.1-15	During identity proofing, the applicant shall be required to provide two forms of identity source documents in original form. The identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1115-0136, Employment Eligibility Verification. At least one document shall be a valid State or Federal government-issued picture identification (ID).	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements

Req#	Requirement	Source	Section Title
1.1-16	The PIV identity proofing, registration and issuance process shall adhere to the principle of separation of duties to ensure that no single individual has the capability to issue a PIV credential without the cooperation of another authorized person.	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements
1.1-17	The identity proofing and registration process used when verifying the identity of the applicant shall be accredited by the department or agency as satisfying the requirements above and approved in writing by the head of the Federal department or agency.	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements
1.1-18	A process for registration and approval must be established, using a method approved by the U.S. Department of State’s Bureau of Diplomatic Security, for citizens of foreign countries who are working for the Federal government overseas, except for employees under the command of a U.S. area military commander.	FIPS 201, Section 2.2	PIV Identity Proofing and Registration Requirements
1.1-19	The issuance and maintenance process used when issuing credentials shall be accredited by the department as satisfying the requirements below and approved in writing by the head of the Federal department or agency.	FIPS 201, Section 2.3	PIV Issuance and Maintenance Requirements
1.1-20	The process shall ensure completion and successful adjudication of a National Agency Check (NAC), National Agency Check with Written Inquiries (NACI), or other OPM or National Security community investigation as required for Federal employment.	FIPS 201, Section 2.3	PIV Issuance and Maintenance Requirements
1.1-21	The PIV credential shall be revoked if the results of the investigation so justify.	FIPS 201, Section 2.3	PIV Issuance and Maintenance Requirements
1.1-22	The system shall, at the time of issuance, verify that the individual to whom the credential is to be issued (and on whom the background investigation was completed) is the same as the intended applicant/recipient as approved by the appropriate authority.	FIPS 201, Section 2.3	PIV Issuance and Maintenance Requirements
1.1-23	The organization shall issue PIV credentials only through systems and providers whose reliability has been established by the agency and so documented and approved in writing (i.e., accredited).	FIPS 201, Section 2.3	PIV Issuance and Maintenance Requirements
1.1-24	Maintain appeals procedures for those who are denied a credential or whose credentials are revoked.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-25	Ensure that only personnel with a legitimate need for access to IIF in the PIV system are authorized to access the IIF, including but not limited to information and databases maintained for registration and credential issuance.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-26	Coordinate with appropriate department or agency officials to define consequences for violating privacy policies of the PIV system.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-27	Assure that the technologies used in the department or agency’s implementation of the PIV system allow for continuous auditing of compliance with stated privacy policies and practices governing the collection, use, and distribution of information in the operation of the program.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-28	Utilize security controls described in NIST SP 800-53, Recommended Security Controls for Federal Information Systems, to accomplish privacy goals, where applicable. [SP800-53].	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-29	Ensure that the technologies used to implement PIV sustain and do not erode privacy protections relating to the use, collection, and disclosure of information in identifiable form. Specifically, employ an electromagnetically opaque sleeve or other technology to protect against any unauthorized contactless access to information stored on a PIV credential.	FIPS 201, Section 2.4	PIV Privacy Requirements

Req#	Requirement	Source	Section Title
1.1-30	Assign an individual to the role of senior agency official for privacy. The senior agency official for privacy is the individual who oversees privacy-related matters in the PIV system and is responsible for implementing the privacy requirements in the standard. The individual serving in this role may not assume any other operational role in the PIV system.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-31	Conduct a comprehensive Privacy Impact Assessment (PIA) on systems containing personal information in identifiable form for the purpose of implementing PIV, consistent with [E-Gov] and [OMB322]. Consult with appropriate personnel responsible for privacy issues at the department or agency (e.g., Chief Information Officer) implementing the PIV system.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-32	Write, publish, and maintain a clear and comprehensive document listing the types of information that will be collected (e.g., transactional information, personal information in identifiable form [IIF]), the purpose of collection, what information may be disclosed to whom during the life of the credential, how the information will be protected, and the complete set of uses of the credential and related information at the department or agency. PIV applicants shall be provided full disclosure of the intended uses of the PIV credential and the related privacy implications.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-33	Assure that systems that contain IIF for the purpose of enabling the implementation of PIV are handled in full compliance with fair information practices as defined in [PRIVACY]. the Privacy Act of 1974 [PRIVACY]	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-34	All departments and agencies shall implement the PIV system in accordance with the spirit and letter of all privacy controls specified in this standard, as well as those specified in Federal privacy laws and policies including but not limited to the E-Government Act of 2002, the Privacy Act of 1974, and OMB Memorandum M-03-22.	FIPS 201, Section 2.4	PIV Privacy Requirements
1.1-35	The PIV Card shall comply with physical characteristics as described in International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 7810 [ISO7810], ISO/IEC 10373 [ISO10373], ISO/IEC 7816 for contact cards [ISO7816], and ISO/IEC 14443 for contactless cards [ISO14443].	FIPS 201, Section 4.1	Physical PIV Card Topology
1.1-36	The printed material shall not rub off during the life of the PIV Card, nor shall the printing process deposit debris on the printer rollers during printing and laminating.	FIPS 201, Section 4.1.1	Physical PIV Card Topology
1.1-37	Printed material shall not interfere with the contact and contactless ICC(s) and related components, nor shall it obstruct access to machine-readable information.	FIPS 201, Section 4.1.1	Physical PIV Card Topology
1.1-38	The PIV Card shall contain security features that aid in reducing counterfeiting, are resistant to tampering, and provide visual evidence of tampering attempts. At a minimum, a PIV Card shall incorporate one such security feature. Examples of these security features include the following: + Optical varying structures + Optical varying inks + Laser etching and engraving + Holograms + Holographic images + Watermarks.	FIPS 201, Section 4.1.2	Tamper Proofing and Resistance

Req#	Requirement	Source	Section Title
1.1-39	Incorporation of security features shall— + Be in accordance with durability requirements ISO7810 + Be free of defects, such as fading and discoloration + Not obscure printed information + Not impede access to machine-readable information.	FIPS 201, Section 4.1.2	Tamper Proofing and Resistance
1.1-40	The PIV Card shall not be embossed.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-41	Decals shall not be adhered to the card.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-42	Departments and agencies may choose to punch an opening in the card body to enable the card to be worn on a lanyard. Departments and agencies should ensure such alterations are closely coordinated with the card vendor and/or manufacturer to ensure the card material integrity is not adversely impacted. Departments and agencies are strongly encouraged to ensure such alterations do not— • Compromise card body durability requirements and characteristics • Invalidate card manufacturer warranties or other product claims • Alter or interfere with printed information, including the photo • Damage or interfere with machine-readable technology, such as the embedded antenna.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-43	The card material shall withstand the effects of temperatures required by the application of a polyester laminate on one or both sides of the card by commercial off-the-shelf (COTS) equipment. The thickness added due to a laminate layer shall not interfere with the smart card reader operation. The card material shall allow production of a flat card in accordance with [ISO7810] after lamination of one or both sides of the card.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-44	The PIV Card shall contain a contact and a contactless ICC interface.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-45	The card body structure shall consist of card material(s) that satisfy the card characteristics in [ISO7810] and test methods in American National Standards Institute (ANSI) 322. [ANSI322] Although the [ANSI322] test methods do not currently specify compliance requirements, the tests shall be used to evaluate card material durability and performance. The [ANSI322] tests minimally shall include card flexure, static stress, plasticizer exposure, impact resistance, card structural integrity, surface abrasion, temperature and humidity-induced dye migration, ultraviolet light exposure, and a laundry test. Cards shall not malfunction or delaminate after hand cleaning with a mild soap and water mixture. The reagents called out in Section 5.4.1.1 of [ISO10373] shall be modified to include a two percent soap solution.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-46	The card shall be subjected to actual, concentrated, or artificial sunlight to appropriately reflect 2000 hours of southwestern United States' sunlight exposure in accordance with [ISO10373], Section 5.12. Concentrated sunlight exposure shall be performed in accordance with [G90-98] and accelerated exposure in accordance with [G155-00]. After exposure, the card shall be subjected to the [ISO10373] dynamic bending test and shall have no visible cracks or failures. Alternatively, the card may be subjected to the [ANSI322] tests for ultraviolet and daylight fading resistance and subjected to the same [ISO10373] dynamic bending test.	FIPS 201, Section 4.1.3	Physical Characteristics and Durability

Req#	Requirement	Source	Section Title
1.1-47	The card shall be 27- to 33-mil thick (before lamination) in accordance with [ISO7810].	FIPS 201, Section 4.1.3	Physical Characteristics and Durability
1.1-48	The information on a PIV Card shall be in visual printed and electronic form.	FIPS 201, Section 4.1.4	Visual Card Topography
1.1-49	Printed data shall not interfere with machine-readable technology.	FIPS 201, Section 4.1.4	Visual Card Topography
1.1-50	Areas that are marked as reserved should not be used for printing.	FIPS 201, Section 4.1.4	Visual Card Topography
1.1-51	The card shall contain mandated printed information.	FIPS 201, Section 4.1.4	Visual Card Topography
1.1-52	The card shall contain mandated machine-readable technologies.	FIPS 201, Section 4.1.4	Visual Card Topography
1.1-53	Mandated and optional items shall generally be placed as described and depicted.	FIPS 201, Section 4.1.4	Visual Card Topography
1.1-54	Zone 1—Photograph. The photograph shall be placed in the upper left corner and be a full frontal pose from top of the head to shoulder, as depicted in Figure 4-1. A minimum of 300 dots per inch (dpi) resolution shall be used. The background should follow recommendations set forth in SP 800-76.	FIPS 201, Section 4.1.4.1	Mandatory Items on the Front of the PIV Card
1.1-55	Zone 2—Name. The full name, or alternatively, pseudonyms as provided under the law, shall be printed directly under the photograph in capital letters. The font shall be a minimum of 10 point.	FIPS 201, Section 4.1.4.1	Mandatory Items on the Front of the PIV Card
1.1-56	Zone 8—Employee Affiliation. A printed employee affiliation shall be printed on the card. Some examples of employee affiliation are “CONTRACTOR,” “ACTIVE DUTY,” and “CIVILIAN.”	FIPS 201, Section 4.1.4.1	Mandatory Items on the Front of the PIV Card
1.1-57	Zone 10— Organizational Affiliation. The Organizational Affiliation shall be printed as depicted in Figure 4-1.	FIPS 201, Section 4.1.4.1	Mandatory Items on the Front of the PIV Card
1.1-58	Zone 14—Expiration Date. The card expiration date shall be printed in a YYYYMMMDD format.	FIPS 201, Section 4.1.4.1	Mandatory Items on the Front of the PIV Card
1.1-59	Zone 1—Agency Card Serial Number. This item shall be printed as depicted in Figure 4-6 and contain the unique serial number from the issuing department or agency. The format shall be at the discretion of the issuing department or agency.	FIPS 201, Section 4.1.4.2	Mandatory Items on the Back of the Card
1.1-60	Zone 2—Issuer Identification. This item shall be printed as depicted in Figure 4-6 and consist of six characters for the department code, four characters for the agency code, and a five-digit number that uniquely identifies the issuing facility within the department or agency.	FIPS 201, Section 4.1.4.2	Mandatory Items on the Back of the Card
1.1-61	Zone 3—Signature. If used, the department or agency shall place the cardholder signature below the photograph and cardholder name as depicted in Figure 4-3. The space for the signature shall not interfere with the contact and contactless placement. Because of card topology space constraints, placement of a signature may limit the size of the optional two-dimensional bar code.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card

Req#	Requirement	Source	Section Title
1.1-62	Zone 4—Agency Specific text area. If used, this area can be used for printing agency specific requirements, such as employee status.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-63	Zone 5—Rank. If used, the cardholder's rank shall be printed in the area as illustrated. Data format is at the department or agency's discretion.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-64	Zone 6—Portable Data File (PDF) Two-Dimensional Bar Code. If used, the PDF bar code placement shall be as depicted in the diagram (i.e., left side of the card). If Zone 3 (a cardholder signature) is used, the size of the PDF bar code may be affected. The card issuer should confirm that a PDF used in conjunction with a PIV Card containing a cardholder signature will satisfy the anticipated PDF data storage requirements.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-65	Zone 9— Header. If used, the text "United States Government" shall be placed as depicted in Figure 4-1. Departments and agencies may also choose to use this zone for other department or agency-specific information, such as identifying a Federal emergency responder role, as depicted in Figure 4-2.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-66	Zone 11—Agency Seal. If used, the seal selected by the issuing department, agency, or organization shall be printed in the area depicted. It shall be printed using the guidelines provided in Figure 4-2 to ensure information printed on the seal is legible and clearly visible.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-67	Zone 12—Footer. The footer is the preferred location for the Emergency Response Official Identification label. If used, a department or agency may print "Federal Emergency Response Official" as depicted in Figure 4-2, preferably in red text. Departments and agencies may also print a secondary line in Zone 9 to further identify the Federal emergency respondent's official role. Some examples of official roles are "Law Enforcement, "Firefighter" and "Emergency Response Team (ERT)".	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-68	Zone 13—Issue Date. If used, the card issuance date shall be printed above the expiration date in YYYYMMMDD format as depicted in Figure 4-2.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-69	Zone 15—Color-Coding for Employee Affiliation. Color-coding may be used for additional identification of employee affiliation. If color-coding is used, it shall be used as a background color for Zone 2 (name) as depicted in Figure 4-4. The following color scheme shall be used for the noted categories: + Blue—foreign nationals + Red—emergency responder officials + Green—contractors. These colors shall be reserved and shall not be employed for other purposes. Zone 15 may be a solid or patterned line at the department or agency's discretion.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card

Req#	Requirement	Source	Section Title
1.1-70	Zone 16—Photo Border for Employee Affiliation. A border may be used with the photo to further identify employee affiliation, as depicted in Figure 4-3. This border may be used in conjunction with Zone 15 to enable departments and agencies to develop various employee categories. The photo border shall not obscure the photo. The border may be a solid or patterned line. For solid and patterned lines, red shall be reserved for emergency response officials, blue for foreign nationals, and green for contractors. All other colors may be used at the department or agency's discretion.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-71	Zone 17—Agency Specific Data. In cases in which other defined optional elements are not used, Zone 17 may be used for other department or agency-specific information, as depicted in Figure 4-5.	FIPS 201, Section 4.1.4.3	Optional Items on the Front of the Card
1.1-72	Zone 3—Magnetic Stripe. If used, the magnetic stripe shall be high coercivity and placed in accordance with [ISO7811], as illustrated in Figure 4-7.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-73	Zone 4—Return To. If used, the "return if lost" language shall be generally placed on the back of the card as depicted in Figure 4-7.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-74	Zone 5—Physical Characteristics of Cardholder. If used, the cardholder physical characteristics (e.g., height, eye color, hair color) shall be printed in the general area illustrated in Figure 4-7.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-75	Zone 6—Additional Language for Emergency Responder Officials. Departments and agencies may choose to provide additional information to identify emergency response officials or to better identify the cardholder's authorized access. If used, this additional text shall be in the general area depicted and shall not interfere with other printed text or machine-readable components. An example of a printed statement is provided in Figure 4-7.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-76	Zone 7—Standard Section 499, Title 18 Language. If used, standard Section 499, Title 18, language warning against counterfeiting, altering, or misusing the card shall be printed in the general area depicted in Figure 4-7.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-77	Zone 8—Linear 3 of 9 Bar Code. If used, a linear 3 of 9 bar code shall be generally placed as depicted in Figure 4-7. It shall be in accordance with Association for Automatic Identification and Mobility (AIM) standards. Beginning and end points of the bar code will be dependent on the embedded contactless module selected. Departments and agencies are encouraged to coordinate placement of the bar code with the card vendor.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-78	Zone 9—Agency-Specific Text. In cases in which other defined optional elements are not used, Zone 9 may be used for other department or agency-specific information, as depicted in Figure 4-8. For example, emergency responder officials may use this area to provide additional details.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-79	In the case of the Department of Defense, the back of the card will have a distinct appearance. This is necessary to display information required by the Geneva Accord and to facilitate medical entitlements that are legislatively mandated.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-80	All text shall be printed using the Arial font.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card

Req#	Requirement	Source	Section Title
1.1-81	Unless otherwise specified, the recommended font size is 5pt normal weight for data labels (also referred to as tags).	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-82	Unless otherwise specified, the recommended font size is 6pt bold for actual data.	FIPS 201, Section 4.1.4.4	Optional Items on the Back of the Card
1.1-83	To support a variety of authentication mechanisms, the PIV logical credentials shall contain multiple data elements for the purpose of verifying the cardholder's identity at graduated assurance levels. These mandatory data elements collectively comprise the data model for PIV logical credentials, and include the following: + A PIN + A CHUID + PIV authentication data (one asymmetric key pair and corresponding certificate) + Two biometric fingerprints.	FIPS 201, Section 4.1.5.1	Logical Credential Data Model
1.1-84	The PIV data model may be optionally extended to meet department or agency-specific requirements. If the data model is extended, this standard establishes requirements for the following four classes of logical credentials: + An asymmetric key pair and corresponding certificate for digital signatures + An asymmetric key pair and corresponding certificate for key management + Asymmetric or symmetric card authentication keys for supporting additional physical access applications + Symmetric key(s) associated with the card management system.	FIPS 201, Section 4.1.5.1	Logical Credential Data Model
1.1-85	The PIV Card must be activated to perform privileged operations such as reading biometric information and using asymmetric keys.	FIPS 201, Section 4.1.6	PIV Card Activation
1.1-86	The PIV Card shall be activated for privileged operations only after authenticating the cardholder or the appropriate card management system.	FIPS 201, Section 4.1.6	PIV Card Activation
1.1-87	PIV Cards shall implement PIN-based cardholder activation to allow privileged operations using PIV credentials held by the card.	FIPS 201, Section 4.1.6.1	Activation by Cardholder
1.1-88	For PIN-based cardholder activation, the cardholder shall supply a numeric PIN.	FIPS 201, Section 4.1.6.1	Activation by Cardholder
1.1-89	The PIN shall be transmitted to the PIV Card and checked by the card. If the presented PIN is correct, the PIV Card is activated.	FIPS 201, Section 4.1.6.1	Activation by Cardholder
1.1-90	The PIV Card shall include mechanisms to limit the number of guesses an adversary can attempt if a card is lost or stolen.	FIPS 201, Section 4.1.6.1	Activation by Cardholder
1.1-91	Moreover, the PIN should not be easily-guessable or otherwise individually-identifiable in nature (e.g., part of a Social Security Number, phone number).	FIPS 201, Section 4.1.6.1	Activation by Cardholder

Req#	Requirement	Source	Section Title
1.1-92	The PIN authentication mechanism shall meet the identity-based authentication requirements of FIPS PUB 140-2 Level 2. [FIPS140-2]	FIPS 201, Section 4.1.6.1	Activation by Cardholder
1.1-93	PIV Cards may support card activation by the card management system to support card personalization and post-issuance card update. To activate the card for personalization or update, the card management system shall perform a challenge response protocol using cryptographic keys stored on the card in accordance with [SP800-73].	FIPS 201, Section 4.1.6.2	Activation by Card Management System
1.1-94	When cards are personalized, card management keys shall be set to be specific to each PIV Card. That is, each PIV Card shall contain a unique card management key.	FIPS 201, Section 4.1.6.2	Activation by Card Management System
1.1-95	Card management keys shall meet the algorithm and key size requirements stated in Special Publication 800-78, Cryptographic Algorithms and Key Sizes for Personal Identity Verification. [SP800-78].	FIPS 201, Section 4.1.6.2	Activation by Card Management System
1.1-96	The PIV Card shall include the CHUID as defined in [SP800-73]. The CHUID includes an element, the Federal Agency Smart Credential Number (FASC-N), which uniquely identifies each card.	FIPS 201, Section 4.2	Cardholder Unique Identifier (CHUID)
1.1-97	The PIV CHUID shall be accessible from both the contact and contactless interfaces of the PIV Card without card activation.	FIPS 201, Section 4.2	Cardholder Unique Identifier (CHUID)
1.1-98	The PIV FASC-N shall not be modified post-issuance.	FIPS 201, Section 4.2	Cardholder Unique Identifier (CHUID)
1.1-99	In addition to the mandatory FASC-N that identifies a PIV Card, the CHUID shall include an expiration date. In machine readable format, the expiration date data element shall specify when the card expires. The expiration date format and encoding rules are as specified in [SP800-73].	FIPS 201, Section 4.2.1	PIV CHUID Data Elements
1.1-100	This standard requires inclusion of the Asymmetric Signature field in the CHUID container. The Asymmetric Signature data element of the PIV CHUID shall be encoded as a Cryptographic Message Syntax (CMS) external digital signature, as defined in RFC 3852 [RFC3852].	FIPS 201, Section 4.2.2	Asymmetric Signature Field in CHUID
1.1-101	The digital signature shall be computed over the entire contents of the CHUID, excluding the Asymmetric Signature field.	FIPS 201, Section 4.2.2	Asymmetric Signature Field in CHUID

Req#	Requirement	Source	Section Title
1.1-102	The issuer asymmetric signature file is implemented as a SignedData Type, as specified in [RFC3852], and shall include the following information: + The message shall include a version field specifying version v3 + The digestAlgorithms field shall be as specified in [SP800-78] + The encapContentInfo shall: – Specify an eContentType of id-PIV CHUIDSecurityObject – Omit the eContent field + The certificates field shall include only a single X.509 certificate which can be used to verify the signature in the SignerInfo field + The crls field shall be omitted + signerInfos shall be present and include only a single SignerInfo + The SignerInfo shall: – Use the issuerAndSerialNumber choice for SignerIdentifier – Specify a digestAlgorithm in accordance with [SP800-78] – Include, at a minimum, the following signed attributes: + A MessageDigest attribute containing the hash computed over the concatenated contents of the CHUID, excluding the asymmetric signature field + A pivSigner-DN attribute containing the subject name that appears in the PKI certificate for the entity that signed the CHUID + Include the digital signature.	FIPS 201, Section 4.2.2	Asymmetric Signature Field in CHUID
1.1-103	The public key required to verify the digital signature shall be provided in the certificates field in an X.509 digital signature certificate issued under [COMMON], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3.	FIPS 201, Section 4.2.2	Asymmetric Signature Field in CHUID
1.1-104	The certificate shall also include an extendedKeyUsage extension asserting id-PIV-content-signing	FIPS 201, Section 4.2.2	Asymmetric Signature Field in CHUID
1.1-105	At a minimum, the PIV Card must store one asymmetric private key and a corresponding public key certificate, and perform cryptographic operations using the asymmetric private key. Cryptographic operations with this key are performed only through the contact interface (GENERAL AUTHENTICATE, GENERATE ASYMMETRIC KEY PAIR command).	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-106	The PIV Card shall implement the following cryptographic operations and support functions: + RSA or elliptic curve key pair generation + RSA or elliptic curve private key cryptographic operations + Importation and storage of X.509 certificates.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-107	The PIV Card may include additional asymmetric keys and PKI certificates.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-108	Where digital signature keys are supported, the PIV Card is not required to implement a secure hash algorithm.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-109	Message hashing may be performed off-card.	FIPS 201, Section 4.3	Cryptographic Specifications

Req#	Requirement	Source	Section Title
1.1-110	Cryptographic operations are not mandated for the contactless interface, but departments and agencies may choose to supplement the basic functionality with storage for a card authentication key and support for a corresponding set of cryptographic operations. For example, if a department or agency wants to utilize Advanced Encryption Standard (AES) based challenge/response for physical access, the PIV Card must contain storage for the AES key and support AES operations through the contactless interface. If the contactless interface utilizes asymmetric cryptography (e.g., elliptic curve cryptography [ECC]), the PIV Card may also require storage for a corresponding public key certificate.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-111	All cryptographic operations using the PIV keys shall be performed on-card; the PIV Card need not implement any additional cryptographic functionality (e.g., hashing, signature verification) by additional cryptographic mechanisms implemented on-card. Algorithms and key sizes for each PIV key type are specified in [SP800-78].	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-112	The PIV authentication key shall be an asymmetric private key supporting card authentication for an interoperable environment, and it is mandatory for each PIV Card.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-113	The card authentication key may be either a symmetric (secret) key or an asymmetric private key for physical access, and it is optional.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-114	The digital signature key is an asymmetric private key supporting document signing, and it is optional.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-115	The key management key is an asymmetric private key supporting key establishment and transport, and it is optional. This can also be used as an encryption key.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-116	All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-117	In addition to an overall validation of Level 2, the PIV Card shall provide Level 3 physical security to protect the PIV private keys in storage.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-118	PIV Authentication Key. This key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the PIV authentication key. The PIV authentication key must be available only through the contact interface of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation)	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-119	The PIV Card shall store a corresponding X.509 certificate to support validation of the public key (for Authentication key). The X.509 certificate shall include the FASC-N in the subject alternative name extension using the pivFASC-N attribute to support physical access procedures. The expiration date of the certificate must be no later than the expiration date of the PIV Card.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-120	Card Authentication Key. The PIV Card shall not permit exportation of the card authentication key. Private/secret key operations may be performed using this key without explicit user action (e.g., the PIN need not be supplied). This standard does not specify key management protocols or infrastructure requirements.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-121	Digital Signature Key. The PIV digital signature key shall be generated on the PIV Card. The PIV Card shall not permit exportation of the digital signature key. If present, cryptographic operations using the digital signature key may only be performed using the contact interface of the PIV Card. Private key operations may not be performed without explicit user action.	FIPS 201, Section 4.3	Cryptographic Specifications

Req#	Requirement	Source	Section Title
1.1-122	The PIV Card shall store a corresponding X.509 certificate to support validation of the digital signature key.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-123	Key Management Key. This key may be generated on the PIV Card or imported to the card. If present, the key management key must only be accessible using the contact interface of the PIV Card. Private key operations may be performed using an activated PIV Card without explicit user action (e.g., the PIN need not be supplied for each operation). This key is sometimes called an encryption key or an encipherment key. The PIV Card shall import and store a corresponding X.509 certificate to support validation of the key management key. Section 5.4 of this document specifies the certificate format and the key management infrastructure for PIV key management keys.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-124	Card Management Key. The card management key is imported onto the card by the issuer. If present, the card management key must only be accessible using the contact interface of the PIV Card.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-125	The PIV Card may also import and store X.509 certificates for use in PKI path validation. These trust anchor certificates may be accessed through the contact interface using an activated PIV Card without explicit cardholder action.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-126	If supported, initialization and update of trust anchor certificates shall require explicit cardholder action, in addition to activation of the card.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-127	The card management key, if present, is a symmetric key used for personalization and post-issuance activities.	FIPS 201, Section 4.3	Cryptographic Specifications
1.1-128	The biometric data used during the PIV Card life cycle activities shall consist of the following: + A full set of fingerprints used to perform law enforcement checks as part of the identity proofing and registration process + An electronic facial image used for printing facial image on the card as well as for performing visual authentication during card usage. A new facial image must be collected at the time of reissuance. The facial image is not required to be stored on the card. + Two electronic fingerprints to be stored on the card for automated authentication during card usage. All three biometric data enumerated above are collected during the identity proofing and registration process. Implementation requirements for storage of biometric data on PIV Cards is dependent on use of specifications contained in NIST SP 800-76 [SP800-76].	FIPS 201, Section 4.4	Biometric Data Specifications
1.1-129	The two electronic fingerprints stored on the card shall be accessible only over the contact interface and after the presentation of a valid PIN.	FIPS 201, Section 4.4	Biometric Data Specifications
1.1-130	No contactless access is permitted for the biometric data specified to be stored on the PIV Card under this standard.	FIPS 201, Section 4.4	Biometric Data Specifications
1.1-131	The full set of fingerprints shall be collected from all PIV Card applicants who can provide them. The technical specifications for the collection and formatting of the ten fingerprints is contained in [SP800-76].	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-132	The fingerprints shall be used for one-to-many matching with the database of fingerprints maintained by the FBI.	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage

Req#	Requirement	Source	Section Title
1.1-133	The fingerprints should be captured using FBI-certified scanners and transmitted using FBI standard transactions.	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-134	A facial image shall be collected from all PIV applicants. The technical specifications for an electronic facial image are contained in [SP800-76].	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-135	The electronic facial image may be used for the following purposes: + For generating the printed image on the card + For generating a visual image on the monitor of a guard workstation for augmenting the visual authentication process defined in Section 6.2.1. This approach may be required in the following situations: – A good live sample of fingerprints cannot be collected from the PIV cardholder due to damage or injury to fingers – Fingerprint matching equipment failure – Authenticating PIV cardholders covered under Section 508.	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-136	Two electronic fingerprints shall be collected from all PIV applicants, who can provide them, for storing on the card. Alternatively, these two electronic fingerprints can also be extracted from the ten fingerprints collected earlier for law enforcement checks. The technical specifications for the two electronic fingerprints are contained in [SP800-76]. The right and left index fingers shall normally be designated as the primary and secondary finger, respectively. However, if those fingers cannot be imaged, the primary and secondary designations shall be taken from the following fingers, in decreasing order of priority: 1. Right thumb 2. Left thumb 3. Right middle finger 4. Left middle finger 5. Right ring finger 6. Left ring finger 7. Right little finger 8. Left little finger	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-137	Even though two fingerprints are available on the card, a department or agency has the option to use one or both of them for the purpose of PIV cardholder authentication. If only one fingerprint is used for authentication, then the primary finger shall be used first. In cases where there is difficulty in collecting even a single fingerprint of acceptable quality, the department or agency shall perform authentication using asymmetric cryptography as described in Section 6.2.4.	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-138	The format for CBEFF_HEADER and the STD_BIOMETRIC_RECORD is specified in [SP800-76].	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-139	The digital signature shall be computed over the entire CBEFF structure except the CBEFF_SIGNATURE_BLOCK itself (which means that it includes the CBEFF_HEADER and STD_BIOMETRIC_RECORD).	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage

Req#	Requirement	Source	Section Title
1.1-140	Agencies shall seek OPM guidance for alternative means for performing law enforcement checks in cases where obtaining ten fingerprints is impossible.	FIPS 201, Section 4.4.1	Biometric Data Collection, Storage, and Usage
1.1-141	The CMS encoding of the CBEFF_SIGNATURE_BLOCK is as a SignedData type, and shall include the following information: + The message shall include a version field specifying version v3 + The digestAlgorithms field shall be as specified in [SP800-78] + The encapcontentInfo shall – Specify an eContentType of id-PIV-biometricObject – Omit the eContent field + If the signature on the biometric was generated with the same key as the signature on the CHUID, the certificates field shall be omitted + If the signature on the biometric was generated with a different key as the signature on the CHUID, the certificates field shall include only a single certificate which can be used to verify the signature in the SignerInfo field + The crls field shall be omitted + signerInfos shall be present and include only a single SignerInfo + The SignerInfo shall – Use the issuerAndSerialNumber choice for SignerIdentifier – Specify a digestAlgorithm in accordance with [SP800-78] Include at a minimum the following signed attributes: + A MessageDigest attribute containing the hash of the concatenated CBEFF_HEADER + STD_BIOMETRIC_RECORD + A pivFASC-N attribute containing the FASC-N of the PIV Card (to link the biometric data and PIV Card) + A pivSigner-DN attribute containing the subject name that appears in the PKI certificate for the entity that	FIPS 201, Section 4.4.2	Biometric Data Representation and Protection
1.1-142	Biometric data shall be stored on the card in a CBEFF structure that contains the representation of the biometric data consists of a CBEFF_HEADER, a STD_BIOMETRIC_RECORD, and a CBEFF_SIGNATURE_BLOCK.	FIPS 201, Section 4.4.2	Biometric Data Representation and Protection
1.1-143	The CBEFF_SIGNATURE_BLOCK shall be encoded as a CMS external digital signature as defined in [RFC3852].	FIPS 201, Section 4.4.2	Biometric Data Representation and Protection
1.1-144	PIV biometric data shall be protected through an authentication mechanism such as a PIN.	FIPS 201, Section 4.4.2	Biometric Data Representation and Protection
1.1-145	An electromagnetically opaque sleeve or other technology shall be used to protect against any unauthorized contactless access to biometric information stored on a contactless IC.	FIPS 201, Section 4.4.2	Biometric Data Representation and Protection
1.1-146	The biometric data content collected over the PIV life cycle shall conform to the specifications outlined in [SP800-76].	FIPS 201, Section 4.4.3	Biometric Data Content
1.1-147	Contact card readers shall conform to the [ISO7816] standard for the card-to-reader interface.	FIPS 201, Section 4.5.1	Contact Reader Specifications

Req#	Requirement	Source	Section Title
1.1-148	These readers shall conform to the Personal Computer/Smart Card (PC/SC) Specification [PCSC] for the reader-to-host system interface in general desktop computing environment.	FIPS 201, Section 4.5.1	Contact Reader Specifications
1.1-149	In physical access control systems where the readers are not connected to general purpose desktop computing systems, the reader-to-host system interface is not specified in this standard.	FIPS 201, Section 4.5.1	Contact Reader Specifications
1.1-150	Contactless card readers shall conform to the [ISO 14443] standard for the card-to-reader interface.	FIPS 201, Section 4.5.2	Contact Reader Specifications
1.1-151	In cases where these readers are connected to general purpose desktop computing systems, they shall conform to [PCSC] for the reader-to-host system interface.	FIPS 201, Section 4.5.2	Contact Reader Specifications
1.1-152	PIN input devices shall be used for implementing PIN-based PIV Card activation.	FIPS 201, Section 4.5.3	PIN Input Device Specifications
1.1-153	When the PIV Card is used with a PIN for physical access, the PIN input device shall be integrated with the reader.	FIPS 201, Section 4.5.3	PIN Input Device Specifications
1.1-154	When the PIV Card is used with a PIN for logical access (e.g., to authenticate to a Web site or other server), the PIN input device may be integrated with the reader or entered using the computer’s keyboard.	FIPS 201, Section 4.5.3	PIN Input Device Specifications
1.1-155	If the PIN input device is not integrated with the reader, the PIN shall be transmitted securely and directly to the PIV Card for card activation.	FIPS 201, Section 4.5.3	PIN Input Device Specifications
1.1-156	Each agency’s PIV implementation(s) shall support interoperability by issuing and managing interoperable PIV Cards and their associated logical credentials specified in Section 4.	FIPS 201, Section 5.1	Control Objectives and Interoperability Requirements
1.1-157	All PIV-II identity proofing and registration systems must satisfy the PIV-I objectives and requirements stated in Section 2.2 in order to be approved.	FIPS 201, Section 5.2	PIV Identity Proofing and Registration Requirements
1.1-158	An additional requirement for PIV-II is that the biometrics (fingerprints and facial image) that are used to personalize the PIV Card must be captured during the identity proofing and registration process.	FIPS 201, Section 5.2	PIV Identity Proofing and Registration Requirements
1.1-159	When issuing PIV Cards, Federal agencies and departments must use an approved identity proofing and registration process. Two approved PIV identity proofing and registration processes are provided in Appendix A. Other identity proofing and registration process may be used if accredited by the department or agency as satisfying the requisite PIV objectives and requirements and approved in writing by the head of the Federal department or agency.	FIPS 201, Section 5.2	PIV Identity Proofing and Registration Requirements
1.1-160	An employee or contractor may be issued PIV Card and logical credentials while a National Agency Check with Written Inquiries (NACI) or other OPM or National Security community investigation required for Federal employment is pending. In such cases, the process must verify successful completion and adjudication of the investigation within six months of PIV card issuance, or the PIV card and the PIV authentication certificate for the card shall be revoked.	FIPS 201, Section 5.3.1	PIV Card Issuance
1.1-161	An additional requirement is that the issuer shall perform a 1:1 biometric match of the applicant against the biometric included in the PIV Card or in the PIV enrollment record. On successful match, the PIV Card shall be released to the applicant.	FIPS 201, Section 5.3.1	PIV Card Issuance

Req#	Requirement	Source	Section Title
1.1-162	The heads of Federal departments and agencies may approve other identity proofing, registration, issuance process sets that are accredited as satisfying the requisite PIV-I objectives and requirements.	FIPS 201, Section 5.3.1	PIV Card Issuance
1.1-163	All PIV-II issuance and maintenance systems shall satisfy the PIV-I objectives and requirements stated in FIPS 201 Section 2.3 in order to be approved.	FIPS 201, Section 5.3.1	PIV Card Issuance
1.1-164	The card issuer shall verify that the employee remains in good standing and personnel records are current before renewing the card and associated credentials. When renewing identity credentials to current employees, the NACI checks shall be followed in accordance with the OPM guidance.	FIPS 201, Section 5.3.2	PIV Card Maintenance
1.1-165	The data and credentials held by the PIV Card may need to be invalidated prior to the expiration date of the card. The cardholder may retire, change jobs, or the employment is terminated, thus requiring invalidation of a previously active card. The card may be damaged, lost, or stolen, thus requiring a replacement. The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder. In this regard, procedures for PIV Card maintenance must be integrated into department and agency procedures to ensure effective card management.	FIPS 201, Section 5.3.2	PIV Card Maintenance
1.1-166	The PIV system must ensure that this information is distributed efficiently within the PIV management infrastructure and made available to parties authenticating a cardholder.	FIPS 201, Section 5.3.2	PIV Card Reissuance
1.1-167	Procedures for PIV Card maintenance shall be integrated into department and agency procedures to ensure effective card management.	FIPS 201, Section 5.3.2	PIV Card Reissuance
1.1-168	The PIV Card shall be valid for no more than five years.	FIPS 201, Section 5.3.2.1	PIV Card Renewal
1.1-169	A cardholder shall be allowed to apply for a renewal starting six weeks prior to the expiration of a valid PIV Card and until the actual expiration of the card.	FIPS 201, Section 5.3.2.1	PIV Card Renewal
1.1-170	The card issuer will verify the cardholder’s identity against the biometric information stored on the expiring card.	FIPS 201, Section 5.3.2.1	PIV Card Renewal
1.1-171	The expired PIV Card must be collected and destroyed.	FIPS 201, Section 5.3.2.1	PIV Card Renewal
1.1-172	The same biometric data may be reused with the new PIV Card while the digital signature must be recomputed with the new FASC-N.	FIPS 201, Section 5.3.2.1	PIV Card Renewal
1.1-173	The expiration date of the PIV authentication certificate and optional digital signature certificate cannot be later than the expiration date of the PIV Card. Hence, a new PIV authentication key and certificate shall be generated.	FIPS 201, Section 5.3.2.1	PIV Card Renewal
1.1-174	If the PIV Card supports the optional key management key, it may be imported to the new PIV Card.	FIPS 201, Section 5.3.2.1	PIV Card Renewal

Req#	Requirement	Source	Section Title
1.1-175	In case of reissuance, the entire registration and issuance process, including fingerprint and facial image capture, shall be conducted.	FIPS 201, Section 5.3.2.2	PIV Card Reissuance
1.1-176	The card issuer shall verify that the employee remains in good standing and personnel records are current before reissuing the card and associated credentials.	FIPS 201, Section 5.3.2.2	PIV Card Reissuance
1.1-177	It is recommended that the old PIV Card, if available, is collected and destroyed. If the card cannot be collected, normal operational procedures shall complete within 18 hours of notification. In some cases, 18 hours is an unacceptable delay. In that case, emergency procedures must be executed to disseminate this information as rapidly as possible. Departments and agencies are required to have procedures in place to issue emergency notifications in such cases.	FIPS 201, Section 5.3.2.2	PIV Card Reissuance
1.1-178	A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged. The cardholder can also apply for reissuance of a valid PIV Card in the event of an employee status or attribute change or if one or more logical credentials have been compromised. When these events are reported, normal operational procedures must be in place to ensure the following: + The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status. + The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. Certificate revocation lists (CRL) issued shall include the appropriate certificate serial numbers. + Online Certificate Status Protocol (OCSP) responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server's internal revocation records).	FIPS 201, Section 5.3.2.2	PIV Card Reissuance
1.1-179	A cardholder shall apply for reissuance of a new PIV Card if the old PIV Card has been compromised, lost, stolen, or damaged.	FIPS 201, Section 5.3.2.2	PIV Card Reissuance
1.1-180	If a PIN reset is performed by the issuer, the card issuer shall ensure that the cardholder's biometric matches the stored biometric on the reset PIV Card before it is provided back to the cardholder.	FIPS 201, Section 5.3.2.3	PIV Card PIN Reset
1.1-181	The PIN on a PIV Card may need to be reset if the contents of the card are locked resulting from the usage of an invalid PIN more than the allowed number of retries stipulated by the department or agency. PIN resets may be performed by the card issuer.	FIPS 201, Section 5.3.2.3	PIV Card PIN Reset
1.1-182	If departments and agencies adopt more stringent procedures for PIN reset (including disallowing PIN reset, and requiring the termination of PIV Cards that have been locked); such procedures shall be formally documented.	FIPS 201, Section 5.3.2.3	PIV Card PIN Reset

Req#	Requirement	Source	Section Title
1.1-183	The termination process is used to permanently destroy or invalidate the use of the card, including the data and the keys on it, such that it cannot be used again. The PIV Card shall be terminated under the following circumstances: + An employee separates (voluntarily or involuntarily) from Federal service + An employee separates (voluntarily or involuntarily) from a Federal contractor + A contractor changes positions and no longer needs access to Federal buildings or systems + A cardholder is determined to hold a fraudulent identity + A cardholder passes away.	FIPS 201, Section 5.3.2.4	PIV Card Termination
1.1-184	Similar to the situation in which the card or a credential is compromised, normal termination procedures must be in place as to ensure the following: + The PIV Card is collected and destroyed. + The PIV Card itself is revoked. Any local databases that indicate current valid (or invalid) FASC-N values must be updated to reflect the change in status. + The CA shall be informed and the certificate corresponding to PIV authentication key on the PIV Card must be revoked. Departments and agencies may revoke certificates corresponding to the optional digital signature and key management keys. CRLs issued shall include the appropriate certificate serial numbers. + OCSP responders shall be updated so that queries with respect to certificates on the PIV Card are answered appropriately. This may be performed indirectly (by publishing the CRL above) or directly (by updating the OCSP server’s internal revocation records). + The IIF that has been collected from the cardholder is disposed of in accordance with the stated privacy and data retention policies of the department or agency.	FIPS 201, Section 5.3.2.4	PIV Card
1.1-185	The CA that issues certificates to support PIV Card authentication shall participate in the hierarchical PKI for the Common Policy managed by the Federal PKI.	FIPS 201, Section 5.4.1	Architecture
1.1-186	Self-signed, self-issued, and CA certificates issued by these CAs shall conform to Worksheet 1: Self-Signed Certificate Profile, Worksheet 2: Self-Issued CA Certificate Profile, and Worksheet 3: Cross Certificate Profile, respectively, in X.509 Certificate and CRL Profile for the Common Policy [PROF].	FIPS 201, Section 5.4.1	Architecture
1.1-187	All certificates issued to support PIV Card authentication shall be issued under the id-CommonHW policy and the id-CommonAuth policy as defined in the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework [COMMON].	FIPS 201, Section 5.4.2	PKI Certificate
1.1-188	CAs and registration authorities may be operated by departments and agencies, or outsourced to PKI service providers.	FIPS 201, Section 5.4.2	PKI Certificate
1.1-189	[COMMON] requires FIPS 140-2 Level 2 validation for the subscriber cryptomodule (i.e., the PIV Card).	FIPS 201, Section 5.4.2	PKI Certificate
1.1-190	In addition, this standard requires the cardholder to authenticate to the PIV Card each time it performs a private key computation with the digital signature key.	FIPS 201, Section 5.4.2	PKI Certificate
1.1-191	[COMMON] specifies the use of RSA along with the key sizes and hash functions.	FIPS 201, Section 5.4.2	PKI Certificate

Req#	Requirement	Source	Section Title
1.1-192	This standard allows additional cryptographic algorithms and key sizes as specified in the [SP 800-78]. Future enhancements to [COMMON] are expected to permit use of additional algorithms. For conformance to this standard, PIV Card management systems are limited to algorithms and key sizes recognized by this standard and the current version of [COMMON].	FIPS 201, Section 5.4.2	PKI Certificate
1.1-193	The required contents of X.509 certificates associated with PIV private keys are based on [PROF]. The relationship is described below: + Authority Information Access (AIA) extensions shall include pointers to the appropriate OCSP status responders, using the id-ad-ocsp access method as specified in Section 8 of [PROF], in addition to the Lightweight Directory Access Protocol (LDAP) Uniform Resource Identifiers (URI) required by [PROF]. + If private key computations can be performed with the PIV authentication key without user intervention (beyond that required for cryptomodule activation), the corresponding certificate must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension. + Certificates containing the public key associated with an asymmetric Card Authentication Key must specify the policy id-CommonAuth instead of id-CommonHW in the certificate policies extension and must assert id-PIV-cardAuth in the extended key usage extension. + Certificates containing the public key associated with a digital signature private key shall conform to Worksheet 5: End Entity Signature Certificate Profile in [PROF]. + Certificates containing the public key associated with a PIV authentication private key shall conform to Worksheet 5: End Entity Signature Certificate Profile in [PROF], but shall not assert the nonRepudiation bit in the keyUsage extension and must include the PIV Card’s FASC-N in the subject alternative name field. + Certificates containing the public key associated with a key management private key shall conform to Worksheet 6: Key Management Certificate Profile in [PROF].	FIPS 201, Section 5.4.2	PKI Certificate
1.1-194	CAs that issue certificates corresponding to PIV private keys shall issue CRLs every 18 hours, at a minimum. The contents of X.509 CRLs shall conform to Worksheet 4: CRL Profile in [PROF].	FIPS 201, Section 5.4.3	X.509 CRL Contents
1.1-195	Departments and agencies whose PKIs have cross-certified with the Federal Bridge CA (FBCA) at Medium-HW, or High Assurance Level may continue to assert department or agency-specific policy Object Identifiers (OID). Certificates issued on or after January 1, 2008 shall assert the id-CommonHW or id-CommonAuth policy OIDs. (Departments and agencies may continue to assert department or agency-specific policy OIDs in addition to the id-CommonHW and id-CommonAuth policy OIDs in certificates issued after January 1, 2008.)	FIPS 201, Section 5.4.4	Migration from Legacy PKIs
1.1-196	The expiration date of the authentication certificate shall not be after the expiration date of the PIV Card. If the card is revoked, the authentication certificate shall be revoked. However, an authentication certificate (and its associated key pair) may be revoked without revoking the PIV Card and may then be replaced. The presence of a valid, unexpired, and unrevoked PIV authentication certificate on a card is proof that the card was issued and is not revoked.	FIPS 201, Section 5.4.5	PKI Repository and OCSP Responder(s) PIV Card
1.1-197	CAs that issue PIV authentication certificates shall maintain a LDAP directory server that holds the CRLs for the certificates it issues, as well as any CA certificates needed to build a path to the Federal Bridge CA.	FIPS 201, Section 5.4.5	PKI Repository and OCSP Responder(s) PIV Card
1.1-198	Certificates shall contain the crlDistributionPoints or authorityInfoAccess extensions needed to locate CRLs and the authoritative OCSP responder.	FIPS 201, Section 5.4.5	PKI Repository and OCSP Responder(s) PIV Card

Req#	Requirement	Source	Section Title
1.1-199	In addition, every CA that issues PIV authentication certificates shall operate an OCSP server that provides certificate status for every authentication certificate the CA issues.	FIPS 201, Section 5.4.5	PKI Repository and OCSP Responder(s) PIV Card
1.1-200	This standard requires distribution of CA certificates and CRLs using LDAP and Hypertext Transport Protocol (HTTP). Specific requirements are found in Table II—Mandatory Repository Service Lightweight Directory Access Protocol (LDAP) Access Requirements of the Shared Service Provider Repository Service Requirements [SSP REP].	FIPS 201, Section 5.4.5.1	Certificate and CRL Distribution
1.1-201	PIV Authentication certificates contain the FASC-N in the subject alternative name extension; hence, these certificates shall not be distributed publicly via LDAP or HTTP.	FIPS 201, Section 5.4.5.1	Certificate and CRL Distribution
1.1-202	When user certificates are distributed, the requirements in Table I—End-Entity Certificate Repository Service Requirements of [SSP REP] shall be satisfied.	FIPS 201, Section 5.4.5.1	Certificate and CRL Distribution
1.1-203	OCSP [RFC2560] status responders shall be implemented as a supplementary certificate status mechanism.	FIPS 201, Section 5.4.5.2	OCSP Status Responders
1.1-204	The OCSP status responders must be updated at least as frequently as CRLs are issued.	FIPS 201, Section 5.4.5.2	OCSP Status Responders
1.1-205	The definitive OCSP responder for each certificate shall be specified in the AIA extension as described in [PROF].	FIPS 201, Section 5.4.5.2	OCSP Status Responders
1.1-206	The PIV Privacy Requirements stated in Section 2.4 apply equally to PIV-II implementations.	FIPS 201, Section 5.5	PIV Privacy Requirements
1.1-207	Parties responsible for controlling access to Federal resources (both physical and logical) shall determine the appropriate level of identity assurance required for access, based on the harm and impact to individuals and organizations as a result of errors in the authentication of the identity of the PIV cardholder.	FIPS 201, Section 6.1	Identity Authentication Assurance Levels
1.1-208	Owners of logical resources shall apply the methodology defined in [OMB404] to identify the level of assurance required for their electronic transaction.	FIPS 201, Section 6.1.1	Relationship to OMB's E-Authentication Guidance
1.1-209	Visual authentication of a PIV cardholder shall be used only to support access control to physical facilities and resources.	FIPS 201, Section 6.2.1	Authentication Using PIV Visual Credentials (VIS)
1.1-210	The PIV Card has several mandatory topographical features on the front and back that support visual identification and authentication, as follows: + Photograph + Name + Employee affiliation employment identifier + Expiration date + Agency card serial number (back of card) + Issuer identification (back of card).	FIPS 201, Section 6.2.1	Authentication Using PIV Visual Credentials (VIS)

Req#	Requirement	Source	Section Title
1.1-211	When a cardholder attempts to pass through an access control point for a Federally controlled facility, a human guard shall perform visual identity verification of the cardholder, and determine whether the identified individual should be allowed through the control point. The series of steps that shall be applied in the visual authentication process are as follows: 1. The human guard at the access control entry point determines whether the PIV Card appears to be genuine and has not been altered in any way. 2. The guard compares the cardholder's facial features with the picture on the card to ensure that they match. 3. The guard checks the expiration date on the card to ensure that the card has not expired. 4. The guard compares the cardholder's physical characteristic descriptions to those of the cardholder. (Optional) 5. The guard collects the cardholder's signature and compares it with the signature on the card. (Optional) 6. One or more of the other data elements on the card (e.g., name, employee affiliation employment identifier, agency card serial number, issuer identification, agency name) are used to determine whether the cardholder should be granted access.	FIPS 201, Section 6.2.1	Authentication Using PIV Visual Credentials (VIS)
1.1-212	The CHUID shall be used for PIV cardholder authentication using the following sequence: 1. The CHUID is read electronically from the PIV Card. 2. The digital signature on the CHUID is checked to ensure the CHUID was signed by a trusted source and is unaltered. (Optional) 3. The expiration date is checked to ensure that the card has not expired. 4. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, Data Universal Numbering System [DUNS]) are used as input to the authorization check to determine whether the cardholder should be granted access.	FIPS 201, Section 6.2.2	Authentication Using the PIV CHUID
1.1-213	The following sequence shall be followed for unattended authentication of the PIV biometric: 1. The CHUID is read from the card. 2. The Expiration Date in the CHUID is checked to ensure the card has not expired. 3. The cardholder is prompted to submit a PIN, activating the PIV Card. 4. The PIV biometric is read from the card. 5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional) 6. The cardholder is prompted to submit a live biometric sample. 7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card. 8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric. 9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access.	FIPS 201, Section 6.2.3.1	Unattended Authentication Using PIV Biometric (BIO)

Req#	Requirement	Source	Section Title
1.1-214	The following sequence shall be followed for attended authentication of the PIV biometric: 1. The CHUID is read from the card. 2. The Expiration Date in the CHUID is checked to ensure that the card has not expired. 3. The cardholder is prompted to submit a PIN. The PIN entry is done in the view of an attendant. 4. The submitted PIN is used to activate the card. The PIV biometric is read from the card. 5. The signature on the biometric is verified to ensure the biometric is intact and comes from a trusted source. (Optional) 6. The cardholder is prompted to submit a live biometric sample. The biometric sample is submitted in the view of an attendant. 7. If the biometric sample matches the biometric read from the card, the cardholder is authenticated to be the owner of the card. 8. The FASC-N in the CHUID is compared with the FASC-N in the Signed Attributes field of the external digital signature on the biometric. 9. One or more of the CHUID data elements (e.g., FASC-N, Agency Code, DUNS) are used as input to the authorization check to determine whether the cardholder should be granted access. This authentication mechanism is similar to the unattended biometric credential check; the only difference is that an attendant (e.g. security guard) supervises the use of the PIV Card and the submission of the PIN and the biometric by	FIPS 201, Section 6.2.3.2	Attended Authentication Using PIV Biometric (BIO)
1.1-215	The PIV Card carries a mandatory asymmetric authentication private key and corresponding certificate, as described in Section 4. The following steps shall be used to perform authentication using the PIV asymmetric authentication key: 1. The cardholder is prompted to submit a PIN. 2. The submitted PIN is used to activate the card. 3. The reader issues a challenge string to the card and requests an asymmetric operation in response. 4. The card responds to the previously issued challenge by signing it using the PIV authentication private key and attaching the associated certificate. 5. The response signature is verified and standards-compliant PKI path validation is conducted. The related digital certificate is checked to ensure that it is from a trusted source. The revocation status of the certificate is checked to ensure current validity. 6. The response is validated as the expected response to the issued challenge. 7. The Subject Distinguished Name (DN) and FASC-N from the authentication certificate are extracted and passed as input to the authorization function.	FIPS 201, Section 6.2.3.2	Attended Authentication Using PIV Biometric (BIO)
1.1-216	It is implicit that an authentication mechanism (Physical access) that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance level.	FIPS 201, Section 6.3.1	Physical Access
1.1-217	The PIV Card may be used to authenticate the cardholder in support of decisions concerning access to logical information resources.	FIPS 201, Section 6.3.2	Logical Access
1.1-218	It is implicit that an authentication mechanism (Logical access) that is suitable for a higher assurance level can also be applied to meet the requirements for a lower assurance	FIPS 201, Section 6.3.2	Logical Access
1.1-219	Funding permitting, NIST will establish detailed criteria that PIV Card issues must meet for accreditation. Additionally, NIST will (again, funding permitting) establish a government-wide program to accredit official issuers of PIV Cards against these accreditation criteria. Until such time as these are completed, agencies must self-certify their own issuers of PIV Cards.	FIPS 201, Appendix B.1	Accreditation of PIV Service Providers

Req#	Requirement	Source	Section Title
1.1-220	In order to accomplish the accreditation of PIV service providers as described above, and to be compliant with the provisions of OMB Circular A-130, App. III, the IT system(s) used by PIV service providers must also be certified in accordance with NIST SP 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems.	FIPS 201, Appendix B.2	Security Certification and Accreditation of IT System(s)
1.1-221	All the cryptographic modules in the PIV system (both on-card and issuer software) shall be validated to FIPS 140-2 with an overall Security Level 2 (or higher).	FIPS 201, Appendix B.4	Cryptographic Testing and Validation (FIPS 140-2 and algorithm standards)
1.1-222	The OID for id-PIV-CHUIDSecurityObject shall be 2.16.840.1.101.3.6.1	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-223	The OID for id-PIV-biometricObject shall be 2.16.840.1.101.3.6.2	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-224	The OID for id-PIV-authCertificateObject shall be 2.16.840.1.101.3.7.1.1.2.2.1	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-225	The OID for PIV Attributes pivCardholder-Name shall be 2.16.840.1.101.3.6.3	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-226	The OID for pivCardholder-DN shall be 2.16.840.1.101.3.6.4	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-227	The OID for pivSigner-DN shall be 2.16.840.1.101.3.6.5	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-228	The OID for pivFASC-N shall be 2.16.840.1.101.3.6.6	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-229	The OID for id-PIV-content-signing shall be 2.16.840.1.101.3.6.7	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension
1.1-230	The OID for id-PIV-cardAuth shall be 2.16.840.1.101.3.6.8	FIPS 201, Appendix D	PIV Object Identifiers and Certificate Extension

Req#	Requirement	Source	Section Title
	SP 800-76-1		
2.1-1	Figure 1 depicts the procedure for fingerprint acquisition and storage.	SP 800-76-1, Section 3.1	Scope
2.1-2	However, if an agency elects to retain images, then they shall be stored in the format specified in section 3.5.	SP 800-76-1, Section 3.2	Fingerprint Data Retention
2.1-3	However, if an agency elects to retain templates, in either proprietary or standardized formats, then they shall be embedded in the [CBEFF] header of section 6.	SP 800-76-1, Section 3.2	Fingerprint Data Retention
2.1-4	A subject's fingerprints shall be collected according to any of the three imaging modes enumerated in Table 1.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-5	For Options 1 and 2 the devices used for capture of the fingerprints shall have been certified by the FBI to conform to Appendix F of the FBI's Electronic Fingerprint Transmission Specification	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-6	For Option 3, a scan of the inked card shall be performed to effect conversion to electronic form. The scanner shall be certified by the FBI as being compliant with [EFTS, Appendix F]	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-7	The native scanning resolution of the device shall be 197 pixels per centimeter (500 pixels per inch) in both the horizontal and vertical directions.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-8	The procedure for the collection of fingerprints, presented in Table 2, shall be followed.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-9	The procedure shall employ the NIST Fingerprint Image Quality [NFIQ] algorithm to initiate any needed reacquisition of the images.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-10	An attending official shall be present at the time of fingerprint capture	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-11	The agency shall employ measures to ensure the quality of acquisition and guard against faulty presentation, whether malicious or unintentional.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-12	In any case, the agency shall ensure that the applicant does not swap finger positions or hands, occlude fingers, or misalign or misplace the fingers.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-13	Although this is not needed with newer, large-platen, devices the official shall in all cases take care to image all fingers completely.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-14	Ordinarily, all ten fingerprints shall be imaged in this process; however, if one or more fingers are not available (for instance, because of amputation) then as many fingers as are available shall be imaged.	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-15	When fewer than ten fingers are collected, the FBI background transaction of Section 3.4 requires (in field AMP 2.084 of an accompanying Type 2 record) the labeling of those fingers that are amputated or otherwise not imaged; see [EFTS, Appendix C].	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-16	Two [MINUSTD] fingerprint templates shall be stored on the PIV Card	SP 800-76-1, Section 3.4.1	Source Images
2.1-17	These shall be prepared from images of the primary and secondary fingers (as specified in [FIPS])	SP 800-76-1, Section 3.4.1	Source Images
2.1-18	These images shall be those obtained by segmenting the plain impressions of the full set of fingerprints captured during PIV Registration and stored in row 8 of Table 2.	SP 800-76-1, Section 3.4.1	Source Images

Req#	Requirement	Source	Section Title
2.1-19	Significant rotation of the multi-finger plain impressions (for example, that which can occur when four fingers are imaged using a narrow platen) shall be removed prior to, or as part of, the generation of the mandatory minutiae templates	SP 800-76-1, Section 3.4.1	Source Images
2.1-20	The rotation angle shall be that which makes the inter-phalangeal creases approximately horizontal or, equivalently, the inter-finger spaces approximately vertical.	SP 800-76-1, Section 3.4.1	Source Images
2.1-21	When a PIV Card is issued, one or more authentication attempts shall be executed per [FIPS, 5.3.1].	SP 800-76-1, Section 3.4.3	Card Issuance
2.1-22	This shall entail capture of new live fingerprints of both the primary and secondary fingers, and matching of those with the PIV Card templates.	SP 800-76-1, Section 3.4.3	Card Issuance
2.1-23	PIV Card templates shall be a conformant instance of the INCITS 378-2004 [MINUSTD] minutiae template standard. That is, the minutiae from both the primary and secondary fingers shall reside within a single INCITS 378 record.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-24	This record shall be wrapped in a single instance of the CBEFF structure specified in Section 6 prior to storage on the PIV Card.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-25	The PIV Card templates shall not be encrypted.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-26	Table 3 is a profile of the generic [MINUSTD] standard. Its specifications shall apply to all minutiae templates placed on PIV Cards.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-27	This document recommends that the minutiae records should be prepared after the images are captured and before they are compressed for storage (see Figure 1).	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-28	Specifically fingerprint images enrolled or otherwise retained by agencies shall be formatted according to the INCITS 381-2004 finger image based interchange format standard [FINGSTD]	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-29	This set shall include ten single-finger images.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-30	These shall be obtained by segmentation of the plain multi-finger images gathered in accordance with Options 1, 2 or 3 of Table 1, and the single plain thumb impressions from presentations 4 & 5 of Options 2 and 3.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-31	These images shall be placed into a single [FINGSTD] record.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-32	The record may also include the associated multi-finger plain impressions and the rolled images.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-33	The record shall be wrapped in the CBEFF structure described in Section 6.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-34	Agencies may encrypt this data per the provisions of Section 6, Table 9, Note 2.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies

Req#	Requirement	Source	Section Title
2.1-35	Rows 1-10 give normative content. Row 11 requires the CBEFF structure of Section 6	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-36	However, its FASC-N value (Table 8, Line 13) may be replaced by a field of all zeroes in this one exceptional case: Storage of PIV registration images before a FASC-N has been assigned.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-37	Such instances (including the digital signature) shall be regenerated once the FASC-N is known	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-38	Images shall either be uncompressed or compressed using an implementation of the Wavelet Scalar Quantization (WSQ) algorithm that has been certified by the FBI. The FBI's current requirement for a 15:1 nominal compression ratio shall apply.	SP 800-76-1, Section 3.5, Normative Note #5	Fingerprint Image format for Images Retained by Agencies
2.1-39	Quality values shall be present. These shall be calculated from the NIST Fingerprint Image Quality (NFIQ) method described in [NFIQ] using the formula Q = 20*(6 - NFIQ).	SP 800-76-1, Section 3.5, Normative Note #8	Fingerprint Image format for Images Retained by Agencies
2.1-40	The quality value shall be set to 254 (the [FINGSTD] code for undefined) if this record is not a single finger print (i.e., it is a multi-finger image, or a palm print) or if the NFIQ implementation fails.	SP 800-76-1, Section 3.5, Normative Note #9	Fingerprint Image format for Images Retained by Agencies
2.1-41	PIV fingerprint images transmitted to the FBI as part of the background checking process shall be formatted according to the ANSI/NIST-ITL 1-2000 standard [FFSMT] and the CJIS-RS-0010 [EFTS] specification.	SP 800-76-1, Section 3.6	Fingerprint Image Specifications for Background Checks
2.1-42	Such records shall be prepared from, and contain, only those images collected as per specifications in Section 3.1.	SP 800-76-1, Section 3.6	Fingerprint Image Specifications for Background Checks
2.1-43	Table 5 enumerates the appropriate transaction formats for the three acquisition options of Section 3.2	SP 800-76-1, Section 3.6	Fingerprint Image Specifications for Background Checks
2.1-44	The FBI documentation [EFTS] should be consulted for definitive requirements.	SP 800-76-1, Section 3.6	Fingerprint Image Specifications for Background Checks
2.1-45	This specification applies to any sensor involved in use of the mandatory PIV Card templates of section 3.4.	SP 800-76-1, Section 4.1	Scope
2.1-46	Fingerprint sensors used for PIV authentication shall conform to the FBI's Image Quality Specifications For Single Finger Capture Devices [SINGFING].	SP 800-76-1, Section 4.2	PIV Authentication Fingerprint Acquisition Specifications
2.1-47	However, if an agency elects to retain them, then they shall be stored in the format specified here.	SP 800-76-1, Section 5.1	Scope
2.1-48	Facial images collected during PIV Registration shall be formatted such that they conform to INCITS 385-2004 [FACESTD].	SP 800-76-1, Section 5.2	Acquisition and format

Req#	Requirement	Source	Section Title
2.1-49	In addition to establishing a format, [FACESTD] specifies how a face image should be acquired.	SP 800-76-1, Section 5.2	Acquisition and format
2.1-50	The images shall be embedded within the CBEFF structure defined in Section 6.	SP 800-76-1, Section 5.2	Acquisition and format
2.1-51	Table 6 is an application profile of [FACESTD] tailored for PIV.	SP 800-76-1, Section 5.2	Acquisition and format
2.1-52	If facial imagery is stored on the PIV Card, the length of the entire record shall fit within the container size limits specified in [800-73].	SP 800-76-1, Section 5.2, Normative Note #1	Acquisition and format
2.1-53	The most recent image shall appear first and serve as the default provided to applications.	SP 800-76-1, Section 5.2, Normative Note #2	Acquisition and format
2.1-54	When facial imagery is stored on the PIV Card, only one image shall be stored.	SP 800-76-1, Section 5.2, Normative Note #3	Acquisition and format
2.1-55	PIV facial images shall conform to the Full Frontal Image Type defined in Section 8 of [FACESTD].	SP 800-76-1, Section 5.2, Normative Note #4	Acquisition and format
2.1-56	Facial image data shall be formatted in either of the compression formats enumerated in Section 6.2 of [FACESTD].	SP 800-76-1, Section 5.2, Normative Note #5	Acquisition and format
2.1-57	Both whole-image and single-region-of-interest (ROI) compression are permitted.	SP 800-76-1, Section 5.2, Normative Note #5	Acquisition and format
2.1-58	This applies when images will be input to automated face recognition products for authentication, and when images are stored on PIV Cards.	SP 800-76-1, Section 5.2, Normative Note #5	Acquisition and format
2.1-59	Facial images shall be compressed using a compression ratio no higher than 15:1.	SP 800-76-1, Section 5.2, Normative Note #6	Acquisition and format
2.1-60	The innermost region should be centered on the face and compressed at no more than 24:1.	SP 800-76-1, Section 5.2, Normative Note #6	Acquisition and format

Req#	Requirement	Source	Section Title
2.1-61	For PIV, faces shall be acquired such that a 20 centimeter target placed on, and normal to, a camera's optical axis at a range of 1.5 meters shall be imaged with at least 240 pixels across it. This ensures that the width of the head (i.e. dimension CC in Figure 8 of [FACESTD]) shall have sufficient resolution for the printed face element of the PIV Card. This specification and Section 8.3.4 of [FACESTD] implies that the image width shall exceed 420 pixels.	SP 800-76-1, Section 5.2, Normative Note #7	Acquisition and format
2.1-62	This resolution specification shall be attained optically without digital interpolation.	SP 800-76-1, Section 5.2, Normative Note #7	Acquisition and format
2.1-63	The distance from the camera to the subject should be greater than or equal to 1.5 meters	SP 800-76-1, Section 5.2, Normative Note #7	Acquisition and format
2.1-64	Facial image data shall be converted to the sRGB color space if it is stored.	SP 800-76-1, Section 5.2, Normative Note #8	Acquisition and format
2.1-65	As stated in Section 7.4.3.3 of [FACESTD] this requires application of the color profile associated with the camera in use.	SP 800-76-1, Section 5.2, Normative Note #8	Acquisition and format
2.1-66	All PIV biometric data shall be embedded in a data structure conforming to Common Biometric Exchange Formats Framework [CBEFF].	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-67	This specifies that all biometric data shall be digitally signed and uniformly encapsulated. This covers: the PIV Card fingerprints mandated by [FIPS]; any other biometric data agencies elect to place on PIV Cards; any biometric records that agencies elect to retain (including purely proprietary, or derivative, elements); and any biometric data retained by, or for, agencies or Registration Authorities.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-68	All such data shall be signed in the same manner as prescribed in [FIPS 201] and [800-73] for the mandatory biometric elements.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-69	The CBEFF Header specified in Table 8 and its notes will be established by NIST as Patron Format "PIV". This format will be established as a formal Patron Format per the provisions of [CBEFF, 6.2].	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-70	All fields of the format are mandatory.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-71	Multi-byte integers shall be in Big Endian byte order.	SP 800-76-1, Section 6, Normative Note #1	Common Header for PIV Biometric Data

Req#	Requirement	Source	Section Title
2.1-72	For the mandatory [MINUSTD] elements on the PIV Card the value shall be b00001101.	SP 800-76-1, Section 6, Normative Note #2	Common Header for PIV Biometric Data
2.1-73	The signature shall be computed over the concatenated CBEFF_HEADER and CBEFF_BIOMETRIC_RECORD in Table 7. This includes the signature block length (on line 4) which may not be known before the signature is computed.	SP 800-76-1, Section 6, Normative Note #3	Common Header for PIV Biometric Data
2.1-74	For fingerprint and facial records defined sections 3.4, 3.5 and 5 the Format Owner shall be 0x001B denoting M1, the INCITS Technical Committee on Biometrics.	SP 800-76-1, Section 6, Normative Note #4	Common Header for PIV Biometric Data
2.1-75	For fingerprint image data defined above the Format Type shall be 0x0401	SP 800-76-1, Section 6, Normative Note #5	Common Header for PIV Biometric Data
2.1-76	For the mandatory fingerprint minutiae data this value shall be 0x0201.	SP 800-76-1, Section 6, Normative Note #5	Common Header for PIV Biometric Data
2.1-77	For face data this value shall be 0x0501.	SP 800-76-1, Section 6, Normative Note #5	Common Header for PIV Biometric Data
2.1-78	For other biometric records on the PIV Card, or otherwise retained by agencies, this field shall be assigned in accordance with the procedures of [CBEFF, 5.2.1.17].	SP 800-76-1, Section 6, Normative Note #5	Common Header for PIV Biometric Data
2.1-79	Creation Date shall be encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ". Each pair of characters (for example, "DD") is coded in 8 bits as an unsigned integer.	SP 800-76-1, Section 6, Normative Note #6	Common Header for PIV Biometric Data
2.1-80	The field "hh" shall code a 24 hour clock value.	SP 800-76-1, Section 6, Normative Note #6	Common Header for PIV Biometric Data
2.1-81	The Validity Period contains two dates each of which shall be coded according to Normative Note 6.	SP 800-76-1, Section 6, Normative Note #7	Common Header for PIV Biometric Data

Req#	Requirement	Source	Section Title
2.1-82	For fingerprint images and any kind of fingerprint template the type shall be 0x000008,	SP 800-76-1, Section 6, Normative Note #8	Common Header for PIV Biometric Data
2.1-83	For facial images the type shall be 0x000002	SP 800-76-1, Section 6, Normative Note #8	Common Header for PIV Biometric Data
2.1-84	For modalities not listed there the value shall be 0x0.	SP 800-76-1, Section 6, Normative Note #8	Common Header for PIV Biometric Data
2.1-85	For the mandatory [MINUSTD] PIV Card templates this value shall be b100xxxxx.	SP 800-76-1, Section 6, Normative Note #9	Common Header for PIV Biometric Data
2.1-86	For single [FINGSTD] fingerprint images or [MINUSTD] templates extracted from them, the quality value shall be Q = 20*(6 - NFIQ) where NFIQ is computed using the method of [NFIQ].	SP 800-76-1, Section 6, Normative Note #10	Common Header for PIV Biometric Data
2.1-87	For all biometric data whether stored on a PIV Card or otherwise retained by agencies the quality value shall be a signed integer between -2 and 100 per the text of INCITS 358.	SP 800-76-1, Section 6, Normative Note #10	Common Header for PIV Biometric Data
2.1-88	A value of -2 shall denote that assignment was not supported by the implementation; a value of -1 shall indicate that an attempt to compute a quality value failed.	SP 800-76-1, Section 6, Normative Note #10	Common Header for PIV Biometric Data
2.1-89	Values from 0 to 100 shall indicate an increased expectation that the sample will ultimately lead to a successful match.	SP 800-76-1, Section 6, Normative Note #10	Common Header for PIV Biometric Data
2.1-90	The zero value required by [FACESTD] shall be coded in this CBEFF field as -2.	SP 800-76-1, Section 6, Normative Note #10	Common Header for PIV Biometric Data
2.1-91	For PIV the Creator field has length 18 bytes of which the first K ≤ 17 bytes shall be printable ASCII characters, and the first of the remaining 18-K shall be a null terminator (zero).	SP 800-76-1, Section 6, Normative Note #11	Common Header for PIV Biometric Data

Req#	Requirement	Source	Section Title
2.1-92	This field shall contain the 25 bytes of the FASC-N component of the CHUID identifier, per [800-73, 1.8.{3,4}].	SP 800-76-1, Section 6, Normative Note #11	Common Header for PIV Biometric Data
2.1-93	That is, this section regulates the test itself, and the testing laboratory, not the products under test, and the data specifications here should not be confused with those given in Section 3 for fielded PIV implementations.	SP 800-76-1, Section 7.1	Scope

Req#	Requirement	Source	Section Title

Card/Reader Interoperability Requirements

Req#	Requirement	Source	Section Title
3-1	The contact interface of the PIV Card shall not require a Programming Voltage to operate correctly.	Interop. Reqs. 2.1.1.1	Card / Reader Interoperability Requirements
3-2	The contact interface of the PIV Card shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002	Interop. Reqs. 2.1.1.2	Card / Reader Interoperability Requirements
3-3	At a minimum, the contact interface of the PIV Card shall support either the T=0 or T=1 transmission protocol as defined in ISO/IEC 7816-3:1997. The card may support both protocols.	Interop. Reqs. 2.1.1.3	Card / Reader Interoperability Requirements
3-4	PIV Cards shall not require the use of any RFU bits in the Global or Specific Interface Bytes to operate correctly.	Interop. Reqs. 2.1.1.4	Card / Reader Interoperability Requirements
3-5	The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001	Interop. Reqs. 2.2.1.1	Card / Reader Interoperability Requirements
3-6	The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001	Interop. Reqs. 2.2.1.2	Card / Reader Interoperability Requirements
3-7	The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001	Interop. Reqs. 2.2.1.3	Card / Reader Interoperability Requirements
3-8	PIV Readers shall not generate a Programming Voltage.	Interop. Reqs. 2.2.2.1	Card / Reader Interoperability Requirements
3-9	PIV readers shall support the Class A operating class as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.	Interop. Reqs. 2.2.2.2	Card / Reader Interoperability Requirements
3-10	The contact interface of the reader shall support both the T=0 and T=1 transmission protocols as defined in ISO/IEC 7816-3:1997	Interop. Reqs. 2.2.2.3	Card / Reader Interoperability Requirements
3-11	PIV Readers shall support implicit protocol and parameter selections as defined in ISO/IEC 7816-3:1997	Interop. Reqs. 2.2.2.4	Card / Reader Interoperability Requirements

Req#	Requirement	Source	Section Title
3-12	The reader-to-host interface for physical access control readers shall conform with one of the following standards: • Ethernet as defined in IEEE 802.3-2005, Standard for Information Technology-Telecommunications and Information Exchange Between Systems • RS-232 as defined in TIA-232, Interface Between Data Terminal Equipment and Data Circuit-Terminating Equipment Employing Serial Binary Data Interchange • RS-485 as defined in TIA-485, Electrical Characteristics of Generators and Receivers For Use in Balanced Digital Multipoint Systems • Wiegand™ as defined in sections 3 and 4 of the SIA Access Control Standard Protocol for the 26-BIT Wiegand™ Reader Interface	Interop. Reqs. 2.2.3.1 through 2.2.3.4	Card / Reader Interoperability Requirements
3-13	Physical access control readers shall read the Agency Code, System Code and Credential Code elements of the FASC-N along with the Expiration Date (YYYYMMDD) from the CHUID as defined by appendix A of NIST Special Publication 800-73. The reader shall output these four elements as concatenated individual binary numbers Parity bits shall be added to the beginning and end of the string providing a total length of 75 bits. The first bit transmitted is the first parity bit, P1, it is even parity calculated over the first 37 code bits. The last bit transmitted is the second parity bit, P2, it is odd parity calculated over the last 36 code bits.	Interop. Reqs. 2.2.3.5	Card / Reader Interoperability Requirements
3-14	Retrieval time for 4 KB of data through the contactless interface of the card shall not exceed 3.0 seconds.	Interop. Reqs. 3.1.1.1	Electronic Authentication Performance Requirements
3-15	Retrieval time for 22 KB of data through the contact interface of the card shall not exceed 2.0 seconds	Interop. Reqs. 3.1.2.1	Electronic Authentication Performance Requirements
3-16	The reader buffer size shall be no less than 256 bytes	Interop. Reqs. 3.2.1	Electronic Authentication Performance Requirements
3-17	The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s), fc/64 (~212 kbits/s), fc/32 (~424 kbits/s) and fc/16 (~847 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005	Interop. Reqs. 3.2.2.1	Electronic Authentication Performance Requirements
3-18	Retrieval time for 4 KB of data through the contactless interface of the reader shall not exceed 3.0 seconds.	Interop. Reqs. 3.2.2.2	Electronic Authentication Performance Requirements
3-19	The PIV reader contact interface shall support the Protocol and Parameters Selection (PPS) protocol as defined in ISO/IEC 7816-3:1997	Interop. Reqs. 3.2.3.1	Electronic Authentication Performance Requirements
3-20	Retrieval time for 22 KB of data through the contact interface of the reader shall not exceed 2.0 seconds	Interop. Reqs. 3.2.3.2	Electronic Authentication Performance Requirements
3-21	Buffers shall not be readable through the contactless interface when the card is stored in an electromagnetically opaque sleeve at any distance	Interop. Reqs. 4.1.1.1	Security Related Requirements
3-22	Buffers shall not be readable through the contactless interface more than 10 cm from the reader	Interop. Reqs. 4.1.1.2	Security Related Requirements

Req#	Requirement	Source	Section Title

Req#	Requirement	Source	Section Title
SP 800-73-1			
4.1-1	The PIV Data Model on the PIV Card must comply with Table 1.	SP 800-73, Section 1.7	PIV Data Model
4.1-2	The Card Capabilities Container shall be identified by data model number “0x10”.	SP 800-73, Section 1.8.1	Card Capability Container
4.1-3	For PIV Cards with dual chip implementations, the CHUID is copied in its entirety between the two chips	SP 800-73, Section 1.8.3	CHUID
4.1-4	In addition to the requirements specified in TIG SCEPACS, the CHUID on a PIV Card shall meet the following requirements: + The Federal Agency Smart Credential Number (FASC-N) shall be consistent with the TIG SCEPACS Option for “System Code || Credential Number” to establish a credential number space of 9,999,999,999 credentials. + The Global Unique Identifier (GUID) field must be present, and may include either an issuer assigned IPv6 address or be coded as all zeros. The GUID is included to enable future migration away from the FASC-N into a robust numbering scheme for all issued credentials. + The DUNS and Organizational Code fields are optional. + The Authentication Key Map is specified as an optional field which enables the application to discover the key reference. This is one method of implementing the symmetric challenge/response protocols using the Card Authentication Key. + The Expiration Date is mapped to the reserved for future use (RFU) tag 0x35, keeping that within the existing scope of the TIG SCEPACS specification. This field shall be 8 bytes in length and shall be encoded as YYYYMMDD. + The CHUID is signed in accordance with FIPS 201. The card issuer’s digital signature key shall be used to	SP 800-73, Section 1.8.3	CHUID
4.1-5	The CBEFF headers shall contain the FASC-N and shall require the Integrity Option.	SP 800-73, Section 1.8.4	Fingerprints
4.1-6	The CBEFF headers shall not require the Confidentiality Option.	SP 800-73, Section 1.8.4	Fingerprints
4.1-7	The security object is in accordance with Appendix C of PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version 1.1.	SP 800-73, Section 1.8.5	Security Object
4.1-8	Tag “0xBA” is used to map the ContainerIDs in the PIV data model to the 16 Data Groups specified in the Machine Readable Travel Document (MRTD).	SP 800-73, Section 1.8.5	Security Object
4.1-9	The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object.	SP 800-73, Section 1.8.5	Security Object
4.1-10	The signature field of the security object shall omit the issuer’s certificate, since it is included in the CHUID.	SP 800-73, Section 1.8.5	Security Object
4.1-11	All FIPS 201 mandatory information printed on the card is duplicated on the chip in this buffer.	SP 800-73, Section 1.9.1	Printed Information Buffer
4.1-12	The Digital Signature key and certificate is for the purpose of document signing. The PKI cryptographic function is protected with a “PIN Always” access rule. This requires cardholder participation every time the key is used for digital signature generation.	SP 800-73, Section 1.9.3	Digital Signature Key

Req#	Requirement	Source	Section Title
4.1-13	The Key Management key and certificate supports the use of encryption for the purpose of confidentiality. This key pair is escrowed by the issuer for key recovery purposes. The PKI cryptographic function is protected with a "PIN" access rule. This requires cardholder activation, but enables multiple compute operations without additional cardholder consent.	SP 800-73, Section 1.9.4	Key Management Key
4.1-14	The Card Authentication key and certificate supports PIV Card Authentication for device to device authentication purposes. Cardholder consent is not required to use this key. The access rule for PKI cryptographic functions is "Always". Where the Card Authentication Key is a symmetric key, the CHUID authentication key map shall be present and specify the cryptographic algorithm and key storage location.	SP 800-73, Section 1.9.5	Card Authentication Key
4.1-15	The following are the requirements that the PIV Card Application places on the ICC platform on which it is implemented or installed: - global security status that includes the security status of a global cardholder PIN - application selection using a truncated AID - ability to reset the security status of an individual application - indication to applications as to which physical communication interface – contact versus contactless – is in use - support for the default selection of an application upon warm or cold reset.	SP 800-73, Section 3.1.1	Platform Requirements
4.1-16	Each command that appears on the card command interface shall be implemented by a card application that is resident in the ICC.	SP 800-73, Section 3.4	Card Applications
4.1-17	Each card application shall have a globally unique name called its AID.	SP 800-73, Section 3.4	Card Applications
4.1-18	The PIX of the AID shall contain an encoding of the version of the card application.	SP 800-73, Section 3.4	Card Applications
4.1-19	The AID of the Personal Identity Verification card application (PIV Card Application) shall be: 'A0 00 00 03 08 00 00 10 00 01 00'	SP 800-73, Section 3.4.1	Personal Identity Verification Card Application
4.1-20	The card platform shall support a default selected card application.	SP 800-73, Section 3.4.2	Default Selected Card Application
4.1-21	Personal identification numbers presented to the card command interface shall be 8 bytes long. If the actual PIN length is less than 8 bytes it shall be padded to 8 bytes with 'FF'.	SP 800-73, Section 3.5.3	Authentication of an Individual
4.1-22	A PIV Card Application shall contain six mandatory data objects for interoperable use and are as follows: 1. Card Capability Container 2. Card Holder Unique Identifier 3. X.509 Certificate for PIV Authentication 4. Card Holder Fingerprint I 5. Card Holder Fingerprint II2 6. Security Object	SP 800-73, Section 4.1	PIV Card Application Data Objects

Req#	Requirement	Source	Section Title
4.1-23	A PIV Card Application shall contain five optional data objects data objects for interoperable use and are as follows: 1. Card Holder Facial Image 2. Printed Information 3. X.509 Certificate for PIV Digital Signature 4. X.509 Certificate for PIV Key Management 5. X.509 Certificate for Card Authentication	SP 800-73, Section 4.1	PIV Card Application Data Objects
4.1-24	For the purpose of constructing PIV Card Application data object names in the CardApplicationURL in CCC of the PIV Card Application, the NIST RID (‘A0 00 00 03 08’) shall be used and the card application type shall be set to ‘00’.	SP 800-73, Section 4.2	OIDs and Tags of PIV Card Application Data Objects
4.1-25	An algorithm identifier shall be a one-byte identifier of a cryptographic algorithm together with a mode of operation and reference data length and compliant with the listing in Table 7 for the cryptographic algorithms that may be recognized on the PIV interfaces.	SP 800-73, Section 5.1	Algorithm Identifier
4.1-26	The default cryptographic algorithm for the PIV Card Application with algorithm identifier '00' is 3 Key Triple DES – ECB.	SP 800-73, Section 5.1	Algorithm Identifier
4.1-27	Upon selection, the PIV Card Application shall return the application property template described in Table 8.	SP 800-73, Section 5.2	Application Property Template
4.1-28	The authenticator BER-TLV used on the PIV client-application programming interface shall have the structure described in Table 10.	SP 800-73, Section 5.3	Authenticator
4.1-29	The connection description BER-TLV used on the PIV client-application programming interface shall have the structure described in Table 11.	SP 800-73, Section 5.4	Connection Description
4.1-30	When represented as a byte, the key reference occupies b8 and b5-b1 while b7 and b6 shall be set to 0. If b8 is 0 then the key reference names global reference data. If b8 is 1 then the key reference names application-specific reference data.	SP 800-73, Section 5.5	Key References
4.1-31	A status word shall be a 2-byte value returned by an entry point on the client-application programming interface or a card command at the card edge.	SP 800-73, Section 5.6	Status Words
4.1-32	A data object shall be identified on the PIV client-application programming interface using its OID. An object identifier on the PIV client-application programming interface shall be a dot delimited string of the integer components of the OID.	SP 800-73, Section 5.7	Object Identifiers
4.1-33	A data object shall be identified on the PIV Card Application card command interface using its BER-TLV tag.	SP 800-73, Section 5.7	Object Identifiers
4.1-34	The PIV Client API shall employ the entry points defined in Section 6.1 to communicate with the PIV Card.	SP 800-73, Section 6.1	Entry Points for Communication
4.1-35	All PIV Card Application card commands shall be supported by a PIV Card Application. Card commands indicated with a 'Yes' in the Command Chaining column in Table 15 shall support command chaining for transmitting a data string too long for a single command as defined in ISO/IEC 7816-4.	SP 800-73, Section 7	Part 3: End-Point PIV Card Application Card Command Interface
4.1-36	The PIV Card Application shall return the status word of ‘6A81’ (Function not supported) when it receives a card command on the contactless interface marked “No” in the Contactless Interface column in Table 15.	SP 800-73, Section 7	Part 3: End-Point PIV Card Application Card Command Interface
4.1-37	The PIV Card Application shall be selected by providing its application identifier 'A0 00 00 03 08 00 00 10 00 01 00’	SP 800-73, Section 7.1.1	SELECT Card Command

Req#	Requirement	Source	Section Title
4.1-38	The complete AID, including the two-byte version, of the PIV Card Application that became the currently selected application upon successful execution of the SELECT command shall be returned in the application property template.	SP 800-73, Section 7.1.1	SELECT Card Command
4.1-39	If the currently selected application is the PIV Card Application when the SELECT APPLICATION command is given and the AID in the data field of the SELECT APPLICATION is neither the AID of the PIV Card Application or the right-truncated version thereof, then the PIV Card Application shall be deselected and all PIV Card Application security status indicators shall be set to FALSE.	SP 800-73, Section 7.1.1	SELECT Card Command
4.1-40	Only key references specific to the PIV Card Application; i.e. local key references, shall be verified by the PIV Card Application VERIFY command.	SP 800-73, Section 7.2.1	VERIFY Card Command
4.1-41	If the current value of the retry counter associated with the key reference is zero, then the comparison shall not be made and the PIV Card Application shall return the status word '69 83'.	SP 800-73, Section 7.2.1	VERIFY Card Command
4.1-42	If the reference data in the VERIFY command data field does not satisfy the criteria in Section 3.5.3, the PIV Card Application shall return the status word '6A 80'.	SP 800-73, Section 7.2.1	VERIFY Card Command
4.1-43	If the VERIFY card command succeeds, then the security status of the key reference shall be set to TRUE and the retry counter associated with the key reference shall be set to the reset retry value associated with the key reference.	SP 800-73, Section 7.2.1	VERIFY Card Command
4.1-44	Only reference data associated with key references specific to the PIV Card Application; i.e. local key references, shall be changed by the PIV Card Application CHANGE REFERENCE DATA command.	SP 800-73, Section 7.2.2	CHANGE REFERENCE DATA Card Command
4.1-45	If the current value of the retry counter associated with the key reference is zero, then the reference data associated with the key reference shall not be changed and the PIV Card Application shall the status word '69 83'.	SP 800-73, Section 7.2.2	CHANGE REFERENCE DATA Card Command
4.1-46	If the CHANGE REFERENCE DATA card command succeeds, then the security status of the key reference shall be set to TRUE and the retry counter associated with the key reference shall be set to the reset retry value associated with the key reference.	SP 800-73, Section 7.2.2	CHANGE REFERENCE DATA Card Command
4.1-47	If the CHANGE REFERENCE DATA card command fails, then the security status of the key reference shall be set to FALSE and the retry counter associated with the key reference shall be decremented by one.	SP 800-73, Section 7.2.2	CHANGE REFERENCE DATA Card Command
4.1-48	If the either the current reference data or the new reference data in the command field of the CHANGE REFERENCE DATA command does not satisfy the criteria in Section 3.5.3, the PIV Card Application shall not change the reference data associated with the key reference and shall return the status word '6A 80'.	SP 800-73, Section 7.2.2	CHANGE REFERENCE DATA Card Command
4.1-49	Only retry counters associated with key references specific to the PIV Card Application; i.e. local key references, shall be reset by the PIV Card Application RESET RETRY COUNTER command.	SP 800-73, Section 7.2.3	RESET RETRY COUNTER Card Command
4.1-50	If the current value of the reset counter associated with the key reference is zero, then retry counter associated with the key reference shall not be reset and the PIV Card Application shall the status word '69 83'.	SP 800-73, Section 7.2.3	RESET RETRY COUNTER Card Command
4.1-51	If the RESET RETRY COUNTER card command succeeds, then the retry counter associated with the key reference shall be set to the reset retry value associated with the key reference. Neither the security status of the key reference or the reset counter shall be changed.	SP 800-73, Section 7.2.3	RESET RETRY COUNTER Card Command

Req#	Requirement	Source	Section Title
4.1-52	If the RESET RETRY COUNTER card command fails, then the security status of the key reference shall be set to FALSE and the reset counter associated with the key reference shall be decremented by one.	SP 800-73, Section 7.2.3	RESET RETRY COUNTER Card Command
4.1-53	If the either the reset retry counter reference data (PUK) or the new reference data (PIN) in the RESET RETRY COUNTER command field of the command does not satisfy the criteria in Section 3.5.3, the PIV Card Application shall not reset the retry counter associated with the key reference and shall return the status word '6A 80'.	SP 800-73, Section 7.2.3	RESET RETRY COUNTER Card Command
4.1-54	The GENERAL AUTHENTICATE command shall be used to authenticate the card or a card application to the client-application (INTERNAL AUTHENTICATE), to authenticate an entity to the card (EXTERNAL AUTHENTICATE), and to perform a mutual authentication between the card and an entity external to the card (MUTUAL AUTHENTICATE).	SP 800-73, Section 7.2.4	GENERAL AUTHENTICATE Card Command
4.1-55	The GENERAL AUTHENTICATE command shall be used to realize the signing functionality on the PIV client-application programming interface.	SP 800-73, Section 7.2.4	GENERAL AUTHENTICATE Card Command
4.1-56	If a card command other than the GENERAL AUTHENTICATICATE command is received by the PIV Card Application before the termination of a GENERAL AUTHENTICATE chain, the PIV Card Application shall rollback to the state it was in immediately prior to the reception of the first command in the interrupted chain.	SP 800-73, Section 7.2.4	GENERAL AUTHENTICATE Card Command
4.1-57	Part 3 compliant cards shall return all the TLV elements of a container in the physical order listed for that container in this data model.	SP 800-73, Appendix A	PIV Data Model
4.1-58	In the single-chip/dual-interface configuration, the PIV Card Application shall be provided the information regarding which interface is in use.	SP 800-73, Appendix A	PIV Data Model
4.1-59	In the dual-chip configuration, a separate PIV Card Application shall be loaded on each chip.	SP 800-73, Appendix A	PIV Data Model
4.1-60	Elements of each data object shall be preceded with the assigned tag as noted in Appendix A of SP 800-73.	SP 800-73, Appendix A	PIV Data Model

4.1-61	The CertInfo byte in certificates identified above shall be encoded as follows:
	`CertInfo::= BIT STRING {`
	`CompressionTypeMsb(0), // 0 = no compression and 1 = gzip compression.`
	`CompressionTypeLsb(1), // shall be set to ‘0’ for PIV Applications`
	`IsX509(2), // shall be set to ‘0’ for PIV Applications`
	`RFU3(3),`
	`RFU4(4),`
	`RFU5(5),`
	`RFU6(6),`
	`RFU7(7)`
	`}`
		SP 800-73, Appendix A	PIV Data Model

Req#	Requirement	Source	Section Title

4-61	The CertInfo byte in certificates identified above shall be encoded as follows:
	CertInfo::= BIT STRING {
	CompressionTypeMsb(0), // 0 = no compression and 1 = gzip compression.
	CompressionTypeLsb(1), // shall be set to ‘0’ for PIV Applications
	IsX509(2), // shall be set to ‘0’ for PIV Applications
	RFU3(3),
	RFU4(4),
	RFU5(5),
	RFU6(6),
	RFU7(7)
	}
		SP 800-73-1, Appendix A	PIV Data Model

Req#	Requirement	Source	Section Title
SP 800-78-1			
5.1-1	Federal departments and agencies must implement these recommendations beginning January 1, 2008.	SP 800-78-1, Section 1.4	Effective Date
5.1-2	PIV Cards must implement private key computations for one or more of the algorithms identified in this section.	SP 800-78-1, Section 2	Application of Cryptography in FIPS 201
5.1-3	Certification Authorities (CAs) and card management systems that protect these objects must support one or more of the cryptographic algorithms, key sizes, and parameters specified in Section 3.2.	SP 800-78-1, Section 2	Application of Cryptography in FIPS 201
5.1-4	Table 3-1 establishes specific requirements for cryptographic algorithms and key sizes for each key type. Table 3-1 also specifies time periods with different sets of acceptable algorithms for each key type.	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-5	Note that 1024 bit RSA is permitted to leverage current products and promote efficient adoption of FIPS 201, but must be phased out by 12/31/2013 for authentication keys and 12/31/2008 for digital signature and key management keys.	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-6	Two key Triple-DES (2TDEA) authentication keys must be phased out by 12/31/2010.	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-7	In addition to the key sizes, keys must be generated using secure parameters.	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-8	Rivest, Shamir, Adleman (RSA) keys must be generated using appropriate exponents, as specified in Table 3-2.	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-9	Adleman (RSA) keys must be generated using appropriate exponents, as specified in Table 3-2. Elliptic curve keys must correspond to one of the following recommended curves from [FIPS186-3]	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-10	To promote interoperability, this specification further limits PIV Authentication and Card Authentication elliptic curve keys to a single curve (P-256).	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-11	Implementations of this specification must choose an exponent greater than or equal to 65,537.	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-12	This specification requires that the key management key must be an RSA key transport key, an Elliptic Curve Diffie-Hellman (ECDH) key, or an elliptic curve Menezes-Qu-Vanstone (MQV) key. The specification for RSA key transport is [PKCS1]; the specification for ECDH and elliptic curve MQV is [SP800-56A].	SP 800-78-1, Section 3.1	PIV Cryptographic Keys
5.1-13	Table 3-3 provides specific requirements for digitally signed information stored on the PIV Card.	SP 800-78-1, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.1-14	For signatures on the CHUID, 800-73 Security Object, and stored biometrics, the hash algorithm that must be used to generate the signature is determined by the signature generation date.	SP 800-78-1, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.1-15	Beginning in 2011, only SHA-256 may be used to generate RSA signatures on PIV objects.	SP 800-78-1, Section 3.2.1	Specification of Digital Signatures on Authentication Information

Req#	Requirement	Source	Section Title
5.1-16	Implementations of this specification [PSS padding scheme] must use the SHA-256 hash algorithm when generating RSA-PSS signatures.	SP 800-78-1, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.1-17	The object identifiers specified in Table 3-4, below, must be used in FIPS 201 implementations to identify the signature algorithm.	SP 800-78-1, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.1-18	FIPS 201 requires generation and storage of an X.509 certificate to correspond with each asymmetric private key contained on the PIV Card.	SP 800-78-1, Section 3.2.2	Specification of Public Keys In X.509 Certificates
5.1-19	Table 3-5, below, specifies the object identifiers that may be used in certificates to indicate the algorithm for a subject public key.	SP 800-78-1, Section 3.2.2	Specification of Public Keys In X.509 Certificates
5.1-20	An additional object identifier must be supplied in a parameters field to indicate the elliptic curve associated with the key. Table 3-6, below, identifies the named curves and associated OIDs.	SP 800-78-1, Section 3.2.2	Specification of Public Keys In X.509 Certificates
5.1-21	This specification requires that the message digests of digital information be computed using the same hash algorithm used in the digital signature used to sign the Security Object.	SP 800-78-1, Section 3.2.3	Specification of Message Digests in the SP 800-73 Security Object
5.1-22	The set of acceptable algorithms depends upon the signature generation date, as specified in Table 3-3.	SP 800-78-1, Section 3.2.3	Specification of Message Digests in the SP 800-73 Security Object
5.1-23	The Security Object format identifies the hash algorithm used when computing the message digests by inclusion of an object identifier; the appropriate object identifiers are identified in Table 3-7.	SP 800-78-1, Section 3.2.3	Specification of Message Digests in the SP 800-73 Security Object
5.1-24	The CRLs and OCSP status responses are digitally signed to support authentication and integrity using a public key and hash algorithm at least as large as that used to sign the certificate.	SP 800-78-1, Section 4	Certificate Status Information
5.1-25	The CRL or OCSP message can also be signed with a larger public key or hash algorithm that satisfies the requirements for signing new PIV information, as specified in Table 3-3.	SP 800-78-1, Section 4	Certificate Status Information
5.1-26	The object identifiers specified in Table 3-4 must be used in CRLs and OCSP messages to identify the signature algorithm.	SP 800-78-1, Section 4	Certificate Status Information
5.1-27	Table 5-1 below, establishes specific requirements for cryptographic algorithms and key sizes for PIV Card Management keys according to the card expiration date.	SP 800-78-1, Section 5	PIV Card Management Keys
5.1-28	Table 6-1 defines the key reference values used on the PIV interfaces.	SP 800-78-1, Section 6.1	Key Reference Values
5.1-29	Table 6-2 lists the algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV interfaces.	SP 800-78-1, Section 6.2	PIV Card Algorithm Identifiers
5.1-30	Table 6-3 summarizes the set of algorithms supported for each key reference value based on the time period of use.	SP 800-78-1, Section 6.3	Algorithm Identifiers for PIV Key Types

Req#	Requirement	Source	Section Title
SP 800-79			
6-1	The Agency has assigned the role of Senior Authorizing Official (SAO).	800-79, Section 2.2	Senior Authorizing Official
6-2	The Senior Agency Official (SAO) shall be responsible for the establishment, budget, and oversight of the PIV functions and services of an agency.	800-79, Section 2.2	Senior Authroizing Official
6-3	The Agency has assigned the role of Designated Accreditation Authority (DAA).	800-79, Section 2.2	Designated Accreditation Authority
6-4	The Designated Accreditation Authority (DAA) shall be a senior agency official with the authority to formally accredit the reliability of PCIs as required by HSPD-12.	800-79, Section 2.2	Designated Accreditation Authority
6-5	The Agency has assigned the role of PCI Manager (may be called an Agency Identity Management Official).	800-79, Section 2.2	PCI Manager
6-6	The PCI Manager (Agency Identity Management Official) shall be responsible for ensuring that all the services specified in FIPS 201 are provided reliably and that PIV Cards are produced and issued in accordance with its requirements.	800-79, Section 2.2	PCI Manager
6-7	The Agency has assigned the role of A Certification Agent (CA).	800-79, Section 2.2	Certification Agent
6-8	A Certification Agent (CA) shall provide a plan to ensure that a realistic assessment of the current reliability of the PCI will be obtained, prior to initiating the activities of the certification process.	800-79, Section 2.2	Certification Agent
6-9	The Agency has assigned the role of PIV Card Applicant Representative	800-79, Section 2.2	PIV Card Applicant Representative
6-10	A PIV Card Applicant Representative shall represent the interests of current or prospective Federal employees and contractors who are the Applicants for PIV Cards.	800-79, Section 2.2	PIV Card Applicant Representative
6-11	The Agency has assigned the role of Agency Official for Privacy (AOP).	800-79, Section 2.2	Agency Official for Privacy
6-12	The role of the Agency Official for Privacy (AOP), defined in FIPS 201, shall not assume any other operational role in the PIV system. The AOP shall be responsible for overseeing privacy-related matters in the PIV system and should work with the PIV Card Applicant Representative to ensure that the rights of Applicants and PIV Subscribers (approved Applicants who have been issued a PIV Card) are protected.	800-79, Section 2.2	Agency Official for Privacy
6-13	There are three accreditation alternative that can be rendered by the DAA: • Authorization to Operate • Interin Authorization to Operate • Denial of Authorization to Operate	800-79, Section 2.3	Accreditation Decisions
6-14	The PCI shall be authorized to perform without restrictions or limitations those services that have been certified as being reliable.	800-79, Section 2.3	Authorization to Operate
6-15	No more than two (2) consecutive Interim Authorizations to Operate shall be granted for a PCI.	800-79, Section 2.3	Interim Authorization to Operate

Req#	Requirement	Source	Section Title
6-16	A PCI shall not be considered accredited during the interim authorization to operate.	800-79, Section 2.3	Interim Authorization to Operate
6-17	If, after reviewing the results of the certification phase assessments, the DAA deems operation of the PCI to be unacceptable, a denial of authorization to operate (DATO) shall be transmitted to the PCI Manager.	800-79, Section 2.3	Denial of Authorization to Operate
6-18	Unless specifically designated otherwise by the DAA, the PCI Manager shall be responsible for the assembly, compilation, and submission of the accreditation package.	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-19	The accreditation package shall contain the following documents: • PCI's operational plan • PCI's assessment reports • PCI's corrective action plan	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-20	The PCI's operations plan shall be prepared by the PCI Manager.	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-21	The PCI's attribute assessment reports shall be prepared by the Certification Agent.	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-22	The PCI's attribute assessment reports shall provide the results of assessing the required attributes of the PCI to determine the extent to which the attributes are exhibited now and expected to continue during future operations.	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-23	The corrective action plan (CAP) is prepared by the PCI Manager	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-24	The corrective action plan (CAP) shall describe the measures that are being implemented— (i) to correct deficiencies noted during the assessment; and (ii) to reduce or eliminate vulnerabilities to the creation and issuance of secure PIV Cards.	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-25	The accreditation decision letter shall contain the following information: • Accreditation decision; • Supporting rationale for the decision; and • Terms and conditions for the authorization.	800-79, Section 2.4	Accreditation Package and Supporting Documentation
6-26	The PCI Manager must have a plan for the design, implementation and operation of the PIV Card issuing System, the performance of the required PIV Card Issuing services, and the management of all required support activities of the organization including certification and accreditation.	800-79, Section 4.1	Planning
6-27	The PCI Manager must be able to create a corrective actions plan to correct any deficiencies discovered in the organization during the certification phase. The Manager must be knowledgeable about the requirements of HSPD-12 and FIPS 201, be organized in having access to the needed documents, and be qualified to carry out all responsibilities of the position.	800-79, Section 4.1	Planning
6-28	The PCI shall be required to collect, organize, store, and disseminate many documents important to its operations.	800-79, Section 4.2	Documentation

Req#	Requirement	Source	Section Title
6-29	The PCI Manager and staff must be knowledgeable of the documentation requirements, including protection of the privacy of the Card Applicants and proper handling of the identity source documents.	800-79, Section 4.2	Documentation
6-30	The PCI must have documented plans which includes the PCI's operational plan and the corrective action plan resulting from certification activities.	800-79, Section 4.2	Documentation
6-31	The PCI must have documented policies which include the PIV Privacy requirements as specified in section 2.4 of FIPS 201 and information security policies relevant to the organization.	800-79, Section 4.2	Documentation
6-32	The PCI must have documented Standards and Guidelines which include all FIPS and NIST Guidelines relevant to the organization as well as international, national, and industry standards applicable to the services and operations of the organization, especially those related to PIV Cards as specified in FIPS 201 and NIST SP 800-73, biometric characteristics of people as specified in NIST SP 800-76, and cryptography as specified in NIST SP 800-78.	800-79, Section 4.2	Documentation
6-33	The PCI must have Identity source documents which state that PIV Card Applicants must supply identity source documents as specified in FIPS 201 so that a PCI can prove that their identity is authentic and can be verified by the originators of the documents. These documents must be stored in a manner that assures that their contents are protected, used only for authorized purposes, and be able to be retrieved at some later time for re-verification if needed.	800-79, Section 4.2	Documentation
6-34	The PCI must have various forms which will be used to obtain information and and reports which will be produced to provide information.	800-79, Section 4.2	Documentation
6-35	The PCI Manager shall implement the operations plan.	800-79, Section 4.3	Implementation
6-36	Personnel, Facilities, Equipment, and procurement shall be assessed during the certification phase of the PCI.	800-79, Section 4.3	Implementation
6-37	The PCI manager shall obtain knowledgable, trustworthy, qualified, reliable and honest people.	800-79, Section 4.3	Personnel
6-38	Adequate facilities are required to house and support - • Personnel, • Storage of vital and sensitive records, • Test systems and associated components (Hardware/software/firmware), and • Other operational components.	800-79, Section 4.3	Facilities
6-39	[The PCI Facility shall ensure that the faility is continually] obtaining adequate and reliable equipment to support the services provided by the PCI.	800-79, Section 4.3	Equipment
6-40	The equipment shall be tested against PIV Card stock to see if it meets FIPS 201 specifications when obtained from the supplier.	800-79, Section 4.3	Equipment
6-41	PIV Card Readers/Writers shall be able to initialize the supplied cards.	800-79, Section 4.3	Equipment
6-42	The biometric data shall be captured from the Applicant and entered into the Integrated Circuit "Chip" memory in the PIV Cards.	800-79, Section 4.3	Equipment
6-43	The required [PIV Card] software, credentials, and data shall be loaded securely.	800-79, Section 4.3	Equipment

Req#	Requirement	Source	Section Title
6-44	The completed PIV Cards shall operate properly when issued.	800-79, Section 4.3	Equipment
6-45	If adequate personnel, facilities, or equipment are not available, they must be procured by the PCI.	800-79, Section 4.3	Procurement
6-46	Procurement must be conducted in a manner that assures that reliable personnel services are obtained and that reliable and conformant equipment is obtained.	800-79, Section 4.3	Procurement
6-47	Documenting PIV System and PCI changes and assessing their potential impact is an essential part of monitoring and maintaining accreditation	800-79, Section 4.4	Operation
6-48	Applicant identity proofing and registration shall be conducted in accordance with Sections 2.2 and 5.2 of FIPS 201-1.	800-79, Section 5.1	Application, Identity Proofing and Registration
6-49	In the Role Based Model, the roles of Applicant, Sponsor, Registrar, and PCI must be played by different people when issuing a PIV Card.	800-79, Section 5.1	Application, Identity Proofing and Registration
6-50	The System Based Model further stipulates that all roles and processes must be provided by accredited service providers compliant with this standard.	800-79, Section 5.1	Application, Identity Proofing and Registration
6-51	A PCI shall implement and support only one approved model, either role based or system based model, at a minimum.	800-79, Section 5.1	Application, Identity Proofing and Registration
6-52	A PCI must interact with the applicant at various times under various circumstances	800-79, Section 5.1	Applicant Interactions
6-53	A PCI must be capable of assuring appropriate privacy to the Applicant and his/her IIF, fairness and consistency in processing PIV Card Applicatitons, and protection of the Integrity and Confidentiality of information in the PIV System	800-79, Section 5.1	Notification of Responsibilities and Rights
6-54	The PCI must be knowledgeable and capable of identity proofing, trustworthy in performing sensitive applicant interviews and background reviews, available and accountable for performing the needed services, and cost effective in providing a potentially time consuming and expensive procedure.	800-79, Section 5.1	Authorization to Conduct Identity Proofing
6-55	The PCI Manager is responsible for ensuring that PIV Cards are designed and produced in accordance with the requirements in FIPS 201 and of the agencies using the PCI’s services.	800-79, Section 5.2	PIV Card Issuance
6-56	During the design and production planning, the PCI must establish the responsibilities and authorities for design and production.	800-79, Section 5.2	PIV Card Issuance
6-57	The PCI is responsible for ensuring that purchased, leased, or created PIV System services comply with FIPS 201 specifications and that similarly acquired PIV Card stock, integrated circuit chips, applications software, communications services and software, and biometric marker (fingerprint and facial images) acquisition equipment conform to relevant standards’ requirements.	800-79, Section 5.2	PIV Card Issuance
6-58	The PCI shall identify, verify, protect and safeguard identity credentials and other personally identifiable information provided for use in initializing or incorporation into the Card.	800-79, Section 5.2	PIV Card Issuance
6-59	The PCI must have the capability and procedures for de-enrolling employees, revoking and destroying Cards, and reissuing Cards, all in compliance with FIPS 201.	800-79, Section 5.2	PIV Card Issuance
6-60	The PCI Manager shall be responsible for ensuring that the monitoring phase of the certification and accreditation processes is undertaken and resources provided to collect and assess relevant evidence of continued reliability of the PCI.	800-79, Section 5.2	PIV Card Issuance

Req#	Requirement	Source	Section Title
6-61	The PCI Manager shall be responsibile for reporting to agency management on the performance of the PIV System and any need for improvement. The Manager is responsible for reviewing the status of the PIV System on a periodic basis to ensure its continuing reliability.	800-79, Section 5.3	PIV Life Cycle Management
6-62	The PCI Manager must obtain and maintain the infrastructure needed to support performing the services required of FIPS 201.	800-79, Section 5.3	PIV Life Cycle Management

SP 800-96

Req#	Requirement	Source	Section Title
7-1	The reader shall be Personal Computer Smart Card (PC/SC) conformant when used with corresponding drivers for the host Operating System Platform.	SP 800-96, Section 2.1.1	Application Programming Interface (API)
7-2	The reader, in conjunction with its corresponding driver, should handle the Application Protocol Data Unit (APDU) exchange with T=0 for case 4 commands (e.g., GET DATA, GENERATE ASYMMETRIC KEY PAIR) by reading all data from the card.	SP 800-96, Section 2.1.1	Application Programming Interface (API)
7-3	the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1	SP 800-96, Section 2.1.2	Application Protocol Data Unit (APDU) Support
7-4	The reader must contain a buffer large enough to receive the maximum size frame permitted by (ISO/IEC) 7816-3, Section 9.4.	SP 800-96, Section 2.1.3	Buffer Size
7-5	PIV Readers shall not generate a Programming Voltage.	SP 800-96, Section 2.1.4	Programming Voltage
7-6	PIV Readers shall support cards with Class A Vccs as defined in ISO/IEC 7816-3:1997 and ISO/IEC 7816-3:1997/Amd 1:2002.	SP 800-96, Section 2.1.5	Support for Operating Class
7-7	Retrieval time1 for 12.5 kilobytes (KB) of data through the contact interface of the reader shall not exceed 2.0 seconds.	SP 800-96, Section 2.1.6	Retrieval Time
7-8	The PIV Reader shall support both the character-based T=0 protocol and block-based T=1 protocol as defined in ISO/IEC 7816-3:1997.	SP 800-96, Section 2.1.7	Transmission Protocol
7-9	The reader shall support Protocol and Parameters Selection (PPS) procedure by having the ability to read character TA1 of the Answer to Reset (ATR) sent by the card as defined in ISO/IEC 7816-3:1997.	SP 800-96, Section 2.1.8	Support for PPS Procedure
7-10	The contact interface of a physical access reader shall support all requirements in sections 2.1.2 to 2.1.8.	SP 800-96, Section 2.2.1	Common Requirements
7-11	The reader shall be Personal Computer Smart Card (PC/SC) conformant when used with corresponding drivers for the host Operating System Platform.	SP 800-96, Section 2.3.1	API
7-12	The reader, in conjunction with its corresponding driver, should handle the Application Protocol Data Unit (APDU) exchange with T=0 for case 4 commands (e.g., GET DATA, GENERATE ASYMMETRIC KEY PAIR) by reading all data from the card.	SP 800-96, Section 2.3.1	API
7-13	the contact interface shall support all card commands for contact based access specified in Section 7, End-point PIV Card Application Card Command Interface of SP 800-73-1	SP 800-96, Section 2.3.2	APDU Support
7-14	The reader must contain a buffer large enough to receive the maximum size frame permitted by (ISO/IEC) 7816-3, Section 9.4.	SP 800-96, Section 2.3.3	Buffer Size
7-15	The PIV Reader shall support parts (1 through 4) of ISO/IEC 14443 as amended in the References of this publication.	SP 800-96, Section 2.3.4	ISO 14443 Support
7-16	The contactless interface of the reader shall support both the Type A and Type B communication signal interfaces as defined in ISO/IEC 14443-2:2001.	SP 800-96, Section 2.3.5	Type A and B Communication Signal Interfaces
7-17	The contactless interface of the reader shall support both Type A and Type B initialization and anti-collision methods as defined in ISO/IEC 14443-3:2001.	SP 800-96, Section 2.3.6	Type A and B Initialization and Anti-Collision

Req#	Requirement	Source	Section Title
7-18	The contactless interface of the reader shall support both Type A and Type B transmission protocols as defined in ISO/IEC 14443-4:2001.	SP 800-96, Section 2.3.7	Type A and B Transmission Protocols
7-19	Retrieval time for 4 KB of data through the contactless interface of the reader shall not exceed 2.0 seconds.	SP 800-96, Section 2.3.8	Retrieval Time
7-20	The contactless interface of the reader shall support bit rates of fc/128 (~106 kbits/s) and fc/32 (~424 kbits/s) as defined in ISO/IEC 14443-3:2001/Amd.1:2005. Bit rates fc), fc/64 (~212 kbits/s), and /64 and fc/32 may be configurable to allow activation / deactivation.	SP 800-96, Section 2.3.9	Transmission Speeds
7-21	The reader shall not be able to read a PIV card more than 10cm from the reader.	SP 800-96, Section 2.3.10	Readability Range
7-22	The contactless interface of a physical access reader shall support all requirements in sections 2.3.2 through 2.3.10.	SP 800-96, Section 2.4.1	Common Requirements

Req#	Requirement	Source	Section Title
SP 800-104			
8-1	All letterings on the PIV Card shall be printed in black except as explicitly stated herein.	SP 800-104, Section 2.1	Zones 15 and 12
8-2	Foreign National color-coding has precedence over Government Employee and Contractor color-coding.	SP 800-104, Section 2.1	Zones 15 and 12
8-3	Foreign National, Government Employee, and Contractor color-coding have precedence over Emergency Response Official color-coding (this implies that Red will never be visible in Zone 15).	SP 800-104, Section 2.1	Zones 15 and 12
8-4	The ERO color-coding, when used, shall be depicted at the footer location of Zone 12 and must print "Emergency Response Official" with white lettering on a red background	SP 800-104, Section 2.1	Zones 15 and 12
8-5	No other color-coding is permitted in Zone 12 when implementing SP 800-104.	SP 800-104, Section 2.1	Zones 15 and 12
8-6	When Zone 15 indicates Foreign National affiliation and the department or agency does not need to highlight ERO status, the footer location of Zone 12 may be used to denote the country or countries of citizenship.	SP 800-104, Section 2.1	Zones 15 and 12
8-7	If so used, the department or agency shall print the country name or the three letter country abbreviation (alpha-3 format) in accordance with ISO 3166-1, Country Codes [ISO 3166].	SP 800-104, Section 2.1	Zones 15 and 12
8-8	Zone 18—Affiliation Color Code. The affiliation color code "B" for Blue or "G" for Green shall be printed in a white circle in Zone 15.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-9	The diameter of the circle shall not be more than 5 mm.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-10	The lettering shall correspond to the printed color in Zone 15.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-11	Zone 19—Expiration Date. The card expiration date shall be printed in a MMMYYYY format in the upper right hand corner.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-12	The expiration date shall be printed in Arial 12pt Bold.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-13	Zone 20—Organizational Affiliation Abbreviation. The organizational affiliation abbreviation may be printed in the upper right hand corner below the date as shown in Figure 1.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-14	If printed, the organizational affiliation abbreviation shall be printed in Arial 12pt Bold.	SP 800-104, Section 2.3	Zones 18, 19, and 20
8-15	Since the card body is white, the white color-coding is achieved by the absence of printing.	SP 800-104, Section 2.4	Color Representation
8-16	Note that [FIPS 201] requires the presence of at least one security feature which may overlap colored or printed regions, thus modifying the perceived color.	SP 800-104, Section 2.4	Color Representation
8-17	In the case of colored regions, the effect of overlap shall not prevent the recognition of the principal color by a person with normal vision (corrected or uncorrected) at a working distance of 50 cm to 200 cm.	SP 800-104, Section 2.4	Color Representation
8-18	White sRGB Tristimulus value {255, 255, 255}	SP 800-104, Section 2.4	Color Representation

Req#	Requirement	Source	Section Title
8-19	White sRGB value {255, 255, 255}	SP 800-104, Section 2.4	Color Representation
8-20	White CMYK value {0, 0, 0, 0}	SP 800-104, Section 2.4	Color Representation
8-21	White Pantone value {White}		
8-22	Green sRGB Tristimulus value {153, 255, 153}	SP 800-104, Section 2.4	Color Representation
8-23	Green sRGB value {203, 255, 203}	SP 800-104, Section 2.4	Color Representation
8-24	Green CMYK value {40, 0, 40, 0}	SP 800-104, Section 2.4	Color Representation
8-25	Green Pantone value {359C}	SP 800-104, Section 2.4	Color Representation
8-26	Blue sRGB Tristimulus value {0, 255, 255}	SP 800-104, Section 2.4	Color Representation
8-27	Blue sRGB value {0, 255, 255}	SP 800-104, Section 2.4	Color Representation
8-28	Blue CMYK value {100, 0, 0, 0}	SP 800-104, Section 2.4	Color Representation
8-29	Blue Pantone value {630C}	SP 800-104, Section 2.4	Color Representation
8-30	Red sRGB Tristimulus value {253, 27, 20}	SP 800-104, Section 2.4	Color Representation
8-31	Red sRGB value {254, 92, 79}	SP 800-104, Section 2.4	Color Representation
8-32	Red CMYK value {0, 90, 86, 0}	SP 800-104, Section 2.4	Color Representation
8-33	Red Pantone value {032C}	SP 800-104, Section 2.4	Color Representation