Req#	Requirement	Source	Section Title
FIPS 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors			
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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 signed the biometric data + Include the digital signature. The X.509 certificate containing the public key required to verify the digital signature shall be issued under [COMMON], and shall meet the format and infrastructure requirements for PIV digital signature keys specified in Section 4.3. The certificate shall also include an extendedKeyUsage extension asserting id-PIV-content-signing. Additional descriptions for the PIV object identifiers are provided in Appendix D.	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.{ [regardless of the orientation of the device while protecting the ICC]. }	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

Req#	Requirement	Source	Section Title
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
1.1-148	{Logical contact card} 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	{Logical contactless card} readers shall conform to PC/SC specification for the reader-to-host system interface in cases where these readers are connected to general purpose desktop computing systems.	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	{If the intended purpose for the reader is 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.	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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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

Req#	Requirement	Source	Section Title
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
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]. + Requirements for algorithms and key sizes for each type of PIV asymmetric key are given in [SP800-78].	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

Req#	Requirement	Source	Section Title
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
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 {(i.e. the reader performs a 1:1 biometric match).}. 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 the cardholder.	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 6.2.4	Authentication using PIV Asymmetric Cryptography (PKI)
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
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)

Req#	Requirement	Source	Section Title
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
1.1-231	{If the reader contains a cryptographic module, it shall be validated to FIPS 140-2. }	Derived from Appendix B.4 FIPS 201-1	Cryptographic Testing and Validation (FIPS 140-2 and algorithm standards)
1.1-232	{Logical PIV Card} readers shall conform to PC/SC specification for the reader-to-host system interface in cases where these readers are connected to general purpose desktop computing systems.	FIPS 201, Section 4.5.2	Contact Reader Specifications

SP 800-76-1: Biometric Data Specification for Personal Identity Verification

2.1-1	If an agency elects to retain images, then they shall be stored in the format specified in section 3.5. The format specification includes the [CBEFF] header of section 6.	SP 800-76-1, Section 3.2	Fingerprint Data Retention
2.1-2	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
2.1-3	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
2.1-4	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 [EFTS, Appendix F].	SP 800-76-1, Section 3.3	Fingerprint Image Acquisition
2.1-5	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 3.2	Fingerprint Image Acquisition
2.1-6	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
2.1-7	All ten fingerprints shall be imaged in the registration 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
2.1-8	The procedure for the collection of fingerprints, presented in Table 2, shall be followed. An attending official shall be present at the time of fingerprint capture.	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	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
2.1-11	Two [MINUSTD] fingerprint templates shall be stored on the PIV Card. 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

Req#	Requirement	Source	Section Title
2.1-12	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
2.1-13	When a PIV Card is issued, one or more authentication attempts shall be executed per [FIPS, 5.3.1].	SP 800-76-1, Section 3.4.2	Card Issuance
2.1-14	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 3.4.2	Card Issuance
2.1-15	PIV Card templates shall be conformant instances of the INCITS 378-2004 [MINUSTD] minutiae template standard as specified in Table 3.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-16	Each finger's template record shall be individually wrapped in the CBEFF structure specified in Section 6 prior to storage on the PIV Card.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-17	The PIV Card templates shall not be encrypted	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-18	The length of the entire fingerprint record shall fit within the container size limits specified in [800-73]. These limits apply to the entire CBEFF wrapped and signed entity, not just the [FINGSTD] record.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-19	Both of the two fields ("Owner" and "Type") of the CBEFF Product Identifier of [MINUSTD, Section 6.4.4] shall be non-zero. The two most significant bytes shall identify the vendor, and the two least significant bytes shall identify the version number of that supplier's minutiae detection algorithm.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-20	The Fingerprint Capture Device ID shall be reported in the minutiae template.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-21	The quality value shall be that computed for the parent fingerprint image using [NFIQ] and reported in the minutiae template as Q = 20*(6 - NFIQ).	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-22	The mandatory card templates shall contain minutiae of type ridge ending or ridge bifurcation. However, for those minutiae where it is not possible to reliably distinguish between a ridge ending and a bifurcation, the category of "other" shall be assigned and encoded using bit values 00b.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-23	All coordinates and angles for minutiae shall be recorded with respect to the original finger image.	SP 800-76-1, Section 3.4.3	Minutia Record
2.1-24	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
2.1-25	Fingerprints 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. 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
2.1-26	There is no restriction on the fingerprint image size. However non-background pixels of the target finger shall be retained (i.e. cropping of the image data is prohibited).	SP 800-76-1, Section 3.5	Fingerprint Image Format for Images Retained by Agencies
2.1-27	If certain fingers cannot be imaged, the value of field 'Number of Images' in the Format for Images Retained by Agencies shall be decremented accordingly.	SP 800-76-1, Section 3.5	Fingerprint Image Format for Images Retained by Agencies
2.1-28	The left and right four-finger images, and two-thumb, images may also be included. The value of field 'Number of Images' in the Format for Images Retained by Agencies shall be incremented accordingly.	SP 800-76-1, Section 3.5	Fingerprint Image Format for Images Retained by Agencies
2.1-29	Fingerprint images in the Format for Images Retained by Agencies 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	Fingerprint Image Format for Images Retained by Agencies
2.1-30	Quality values in the Format for Images Retained by Agencies shall be present in the field 'Finger image quality'. 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	Fingerprint Image Format for Images Retained by Agencies

Req#	Requirement	Source	Section Title
2.1-31	The quality value for 'Finger image quality' shall be set to 254 (the [FINGSTD] code for undefined) if this record is not a single fingerprint (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	Fingerprint Image Format for Images Retained by Agencies
2.1-32	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
2.1-33	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
2.1-34	Facial images collected during PIV Registration shall be formatted such that they conform to INCITS 385-2004 [FACESTD] as outlined in Table 6.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-35	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	Acquisition and Format
2.1-36	When facial imagery is stored on the PIV Card, only one image shall be stored.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-37	If more than one image is stored in the record, the most recent image shall appear first and serve as the default provided to applications.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-38	Facial image data shall be formatted in either of the compression formats enumerated in Section 6.2 of [FACESTD]. Both whole-image and single-region-of-interest (ROI) compression are permitted.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-39	Facial images shall be compressed using a compression ratio no higher than 15:1.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-40	Facial images need to conform to the application profile of INCITS 385-2004 tailored for PIV as outlined in Table 6 – “INCITS 385 Profile for PIV Facial Images”.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-41	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.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-42	The Facial resolution specification shall be attained optically without digital interpolation.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-43	Facial image data shall be converted to the sRGB color space if stored. According to Section 7.4.3.3 of INCITS 385-2004 this requires application of the color profile associated with the camera in use.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-44	PIV facial images shall conform to the Full Frontal Image Type defined in Section 8 of INCITS 385-2004.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-45	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.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-46	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
2.1-47	The CBEFF Header conforms to INCITS 398 Section 5.2.1 and contains the added FIPS data types found in Table 8.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-48	For Patron Format PIV Specification, the Creator field has length 18 bytes of which the first K ≤ 17 bytes shall be ASCII characters, and the first of the remaining 18-K shall be a null terminator (zero).	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-49	For Patron Fomrat PIV Specification, the FASC-N 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	Common Header for PIV Biometric Data
2.1-50	The security options field in the Patron Format PIV Specification shall be b00001101 for mandatory elements on the PIV Card.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-51	For fingerprint and facial records defined in § 6 NN#2, the Format Owner shall be 0x001B denoting M1, the INCITS Technical Committee on Biometrics. Otherwise see [CBEFF, 5.2.1.17].	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-52	For Patron Format PIV Specification, fingerprint image data defined in the Format Type shall be 0x0401. For the mandatory fingerprint minutiae template data this value shall be 0x0201. For face data this value shall be 0x0501.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data

Req#	Requirement	Source	Section Title
2.1-53	For Patron Format PIV Specification, other biometric records on the PIV Card or otherwise retained by agencies, the Format Type field shall be assigned in accordance with the procedures of [CBEFF, 5.2.1.17].	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-54	For Patron Format PIV Specification, the Creation Date shall be encoded in eight bytes using a binary representation of "YYYYMMDDhhmmssZ".	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-55	For Patron Format PIV Specification, the Validity Period contains two dates each of which shall be coded as UTC Time.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-56	For Patron Format PIV Specification, fingerprint images and any kind of fingerprint template the type shall be 0x000008, for facial images the type shall be 0x000002. The value for other biometric modalities shall be that given in [CBEFF, 5.2.1.5]. For modalities not listed there the value shall be 0x0.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-57	The Patron Format PIV Specification Biometric Data Type field shall be populated in accordance to Table 9, asserting the degree to which biometric data has been processed.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-58	The CBEFF Biometric Data Type field encoding shall adhere to SP 800-76, Table 9 to convey the degree to which the biometric data has been processed. For templates located on a PIV card, this value shall be b100xxxxx.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-59	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. 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. Values from 0 to 100 shall indicate an increased expectation that the sample will ultimately lead to a successful match. The zero value required by [FACESTD] shall be coded in this CBEFF field as -2	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-60	Interoperability testing requires exchange of templates between products, which shall therefore be tested as a group.	SP 800-76-1, Section 7.3	Test Overview
2.1-61	The certification procedure shall be conducted offline. This allows products to be certified using very large biometric data sets, in repeatable, deterministic and therefore auditable evaluations.	SP 800-76-1, Section 7.3	Test Overview
2.1-62	A template generator shall be certified as a software library. For PIV, a template generator is a library function that shall convert an image into a minutiae record.	SP 800-76-1, Section 7.3.1	Template Generator
2.1-63	A supplier's implementation, submitted for certification, shall satisfy the requirements of an application programming interface (API) specification to be published by the test organizer. The API specification will require the template generator to accept image data and produce [MINUSTD] templates conformant to Table 10.	SP 800-76-1, Section 7.3.1	Template Generator
2.1-64	The CBEFF header and CBEFF signature shall not be included.	SP 800-76-1, Section 7.3.1	Template Generator
2.1-65	The testing laboratory shall input images to the generator using either the Option A or Option B data element specifications given in Table 10. The input data shall be prepared by the testing laboratory.	SP 800-76-1, Section 7.3.1	Template Generator
2.1-66	A template matcher shall be certified as a software library. For PIV, a matcher is a software function that compares enrollment templates with authentication templates to produce a similarity score.	SP 800-76-1, Section 7.3.2	Template matcher
2.1-67	The similarity score must be an integer or real value quantity.	SP 800-76-1, Section 7.3.2	Template matcher
2.1-68	A supplier's implementation, submitted for certification, shall satisfy the API specification published by the test organizer.	SP 800-76-1, Section 7.3.2	Template matcher
2.1-69	Both authentication template and enrollment template shall conform to the Table 11 profile of [MINUSTD].	SP 800-76-1, Section 7.3.2	Template matcher
2.1-70	The test shall neither prescribe nor prohibit methods whereby fingers' material shall be employed in the core comparison. The only constraint is that all invocations of the matching function shall yield a similarity score regardless of the input templates.	SP 800-76-1, Section 7.3.2	Template matcher
2.1-71	The testing laboratory shall publish a test specification document. This document shall establish deadlines for submission of products for certification.	SP 800-76-1, Section 7.4	Test Procedure
2.1-72	The supplier of a template generator shall submit a request for certification to the testing laboratory.	SP 800-76-1, Section 7.4	Test Procedure

Req#	Requirement	Source	Section Title
2.1-73	The testing laboratory shall provide a set of samples to these suppliers. This set shall support debugging and shall consist of images conformant to either the A or B specifications of Table 10. The supplier shall submit templates from this data to the testing laboratory. The supplier shall submit the template generator to the testing laboratory.	SP 800-76-1, Section 7.4	Test Procedure
2.1-74	The testing laboratory shall execute it and check that it produces identical templates to those submitted by the supplier. The testing laboratory shall apply a conformance assessor to the templates. The testing laboratory shall report to the supplier whether identical templates were produced and whether the templates are conformant to the specifications in Table 11.	SP 800-76-1, Section 7.4	Test Procedure
2.1-75	The supplier of a template matcher shall submit a request for certification to the testing laboratory.	SP 800-76-1, Section 7.4	Test Procedure
2.1-76	The testing laboratory shall provide a set of samples to these suppliers. This set shall support debugging and shall consist of images conformant to either the A or B specifications of Table 10 and templates conformant to the specification of Table 11. The supplier shall submit similarity scores from this data to the testing laboratory. The supplier shall submit the template matcher to the testing laboratory.	SP 800-76-1, Section 7.4	Test Procedure
2.1-77	The testing laboratory shall execute it and check that it produces identical scores to those submitted by the supplier. The testing laboratory shall report to the supplier the result of the check.	SP 800-76-1, Section 7.4	Test Procedure
2.1-78	The testing laboratory shall apply all template generators to the first biometric sample from each member of the test corpus. The testing laboratory shall invoke all template matchers to compare the resulting enrollment templates with second authentication templates from each member of the corpus. The authentication template shall be generated by the matcher supplier's generator (i.e. not by another supplier's generator). This shall be done for all pair wise combinations of template generators and template matchers. The result is a set of genuine similarity scores for each combination.	SP 800-76-1, Section 7.4	Test Procedure
2.1-79	The testing laboratory shall invoke all template matchers to compare enrollment templates with second authentication templates from members of a disjoint population. The authentication template shall, in all cases, be generated by the matcher supplier's generator. This shall be done for all pair wise combinations of template generators and template matchers. The result is a set of impostor similarity scores for each combination. The order in which genuine and impostor similarity scores are generated shall be randomized (i.e. it is not implied by the order of the last two paragraphs).	SP 800-76-1, Section 7.4	Test Procedure
2.1-80	The testing laboratory shall sum the similarity score obtained from matching of the image of a primary finger with that obtained from matching of the image of a secondary finger. This sum-rule fusion represents two-finger authentication.	SP 800-76-1, Section 7.4	Test Procedure
2.1-81	The testing laboratory shall compute the detection error tradeoff characteristic (DET) for all pair wise combinations of the template generators and template matchers.	SP 800-76-1, Section 7.5	Determination of an Interoperable Group
2.1-82	The testing laboratory shall generate a rectangular interoperability matrix (see [ISOSWAP]). The matrix has rows corresponding to the generators and columns corresponding to the matchers. Each element of the interoperability matrix shall be the false reject rate at a fixed false accept rate. This value corresponds to one operating point on the DET.	SP 800-76-1, Section 7.5	Determination of an Interoperable Group
2.1-83	An interoperable group of template generators and matchers shall be established as the largest subgroup of products submitted in an initial certification round for which all elements of the interoperability sub-matrix (i.e. FRR values) are less than or equal to 1% at a fixed 1% FAR operating point.	SP 800-76-1, Section 7.5	Determination of an Interoperable Group
2.1-84	Images shall be conformant to this specification if: 1. The acquisition procedures of 3.2 are followed. This may be tested by human observation. 2. The images are conformant to [FINGSTD] as profiled by Table 4 and its normative notes.	SP 800-76-1, Section 8.2	Conformance to PIV Registration Fingerprint Acquisition Specifications
2.1-85	Conformance shall be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 3. Performance certification according to Section 7 is necessary.	SP 800-76-1, Section 8.3	Conformance of PIV Card Fingerprint Template Records
2.1-86	Conformance shall be tested by inspection of the records and performing the test assertions of the "PIV Conformance" column of Table 4. Quality values [NFIQ] shall be checked against the NIST reference implementation.	SP 800-76-1, Section 8.4	Conformance of PIV Registration Fingerprints Retained by Agencies

Req#	Requirement	Source	Section Title
2.1-87	These shall be tested by inspection of the transactions submitted to the FBI. This inspection may be performed either by capturing the transactions at the submitting agency or at the FBI.	SP 800-76-1, Section 8.5	Conformance of PIV Background Check Records
2.1-88	Conformance to Section 4.2 shall be achieved if certification according to [SINGFING] is achieved, and if the resolution and area specifications are met. The [SINGFING] certification process entails inspection of output images.	SP 800-76-1, Section 8.6	Conformance to PIV Authentication Fingerprint Acquisition Specifications
2.1-89	Conformance to Section 5 shall be achieved by conformance to all the normative content of the section. This includes production of records conformant to [FACESTD] as profiled in Section 5.2. Conformance shall be tested by inspection of records and performing the test assertions of the "PIV Conformance" column of Table 6.	SP 800-76-1, Section 8.7	Conformance of PIV Facial Image Records
2.1-90	Conformance of PIV Facial image Records shall be achieved by conformance to all the normative content of Section 5. This includes production of records conformant to [FACESTD] as profiled in Section 5.2.	SP 800-76-1, Section 8.7	Conformance of PIV Facial Image Records
2.1-91	A PIV implementation will be conformant to section 6 if all biometric data records, whether or not mandated by this document or [FIPS], are encapsulated in conformant CBEFF records.	SP 800-76-1, Section 8.8	Conformance of CBEFF Wrappers
2.1-92	CBEFF records are conformant if: 1. the fields of the Table 8 header are present; 2. the fields of Table 8 contain the allowed values as governed by its normative notes; 3. a digital signature conformant to [800-78] is present; 4. the values are consistent with the enclosed biometric data and the trailing digital signature.	SP 800-76-1, Section 8.8	Conformance of CBEFF Wrappers
2.1-93	A template generator shall be certified if: 1. it converts all input Table 10 [FINGSTD] instances to Table 11 [MINUSTD] templates and these pass the template conformance test suite established by NIST, and 2. it converts 90% of Table 10 [FINGSTD] instances in fewer than 1.3 seconds4 each, and 3. all certified matchers verify its output templates with FRR less than or equal to 1% at a FAR of 1%.	SP 800-76-1, Section 8.9	Conformance of Template Generators
2.1-94	A template matcher shall be certified if: 1. it converts all input Table 11 [MINUSTD] templates to scalar scores, and 2. it executes 90% of the Section 7.4 template matches in fewer than 0.1 seconds each, and 3. it matches templates from all certified template generators, and the template generator accompanying the matcher, with FRR less than or equal to 1% at a FAR of 1%.	SP 800-76-1, Section 8.10	Conformance of Template Matchers
2.1-95	The rotation angle shall be that which makes the inter-phalangeal creases approximately horizontal or, equivalently, the inter-finger spaces approximately vertical. This requirement supports interoperable fingerprint matching	SP 800-76-1, Section 3.4.1	Source Images
2.1-96	The fingerprint set shall include ten single-finger images.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-97	The fingerprint images shall be placed into a single [FINGSTD] record.	SP 800-76-1, Section 3.5	Fingerprint Image format for Images Retained by Agencies
2.1-98	Facial image width shall exceed 420 pixels.	SP 800-76-1, Section 5.2	Acquisition and Format
2.1-99	All such data shall be signed in the same manner as prescribed in [FIPS 201] and [800-73] for the mandatory biometric elements. The signature is present in for integrity and shall be stored in the CBEFF signature block. The overall arrangement is depicted in table 7	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-100	The CBEFF Header conforms to INCITS 398 Section 5.2.1 and contains the added FIPS data types found in Table 8. All fields of the format are mandatory.	SP 800-76-1, Section 6	Common Header for PIV Biometric Data
2.1-101	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
2.1-102	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
2.1-103	The test specification shall require that template generators produce a conformant template regardless of the input. Such a template may contain zero minutiae.	SP 800-76-1, Section 7.3.1	Template Generator
2.1-104	It is recommended that a template generator submitted for testing should deprecate any internal quality acceptance mechanism, and attempt production of a viable template.	SP 800-76-1, Section 7.3.1	Template Generato
2.1-105	The input [MINUSTD] enrollment templates shall be prepared by the test agent using software from a supplier.	SP 800-76-1, Section 7.3.2	Template Matcher
2.1-106	The input [MINUSTD] authentication templates shall be the output of the template generation software provided by the supplier of the matcher under test.	SP 800-76-1, Section 7.3.2	Template Matcher
Card/Reader Interoperability Requirements			
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. 2.1.1.1	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. 2.2.2.1	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. 2.2.2.2	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. 2.2.2.3	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. 4.2.1.1	Security Related Requirements
3-22	Buffers shall not be readable through the contactless interface more than 10 cm from the reader	Interop. Reqs. 4.2.1.1	Security Related Requirements

SP 800-73-3: Interfaces for Personal Identity Verification [see Note 3 below]

4.3-1	A PIV Card Application shall contain five mandatory interoperable data objects. The five mandatory data objects for interoperable use are as follows: 1. Card Capability Container 2. Card Holder Unique Identifier 3. X.509 Certificate for PIV Authentication 4. Cardholder Fingerprints 5. Security Object	SP 800-73-3, Part 1, Section 3	End Point PIV Data Model Elements

Req#	Requirement	Source	Section Title
4.3-2	A PIV Card Application may contain twenty-eight optional interoperable data objects. The twenty-eight optional data objects for interoperable use are as follows: 1. Cardholder Facial Image 2. Printed Information 3. X.509 Certificate for Digital Signature 4. X.509 Certificate for Key Management 5. X.509 Certificate for Card Authentication 6. Discovery Object 7. Key History Object 8. 20 retired X.509 Certificates for Key Management 9. Cardholder Iris Images	SP 800-73-3, Part 1, Section 3	End Point PIV Data Model Elements
4.3-3	The Card Capabilities Container shall be identified by data model number “0x10”.	SP 800-73-3, Part 1, Section 3.1.1	Card Capability Container
4.3-4	For {PIV Cards with} dual chip implementations, the CHUID is copied in its entirety between the two chips	SP 800-73-3, Part 1, Section 3.1.2	CHUID
4.3-5	In addition to the requirements specified in TIG SCEPACS, the CHUID on the PIV Card shall meet the following requirements: + The Buffer Length field is an optional TLV element. This element is the length in bytes of the entire CHUID, excluding the Buffer Length element itself, but including the CHUID's Asymmetric Signature element. The calculation of the asymmetric signature must exclude the Buffer Length element if it is present. + The Federal Agency Smart Credential Number (FASC-N) shall be in accordance with TIG SCEPACS [4]. A subset of the FASC-N, the FASC-N Identifier, shall be the unique identifier as described in [4, 6.6]: “The combination of an Agency Code, System Code, and Credential Number is a fully qualified number that is uniquely assigned to a single individual”. The Agency Code is assigned to each Department or Agency by Special Publication 800-87 (SP 800-87), Codes for Identification of Federal and Federally-Assisted Organizations [5]. The subordinate System Code and Credential Number value assignment is subject to Department or Agency policy, provided that the FASC-N identifier (i.e., the concatenated Agency Code, System Code, and Credential Number) is unique for each card. The same FASC-N value shall be used in all the PIV data objects that include the FASC-N. To eliminate unnecessary use of the SSN , the FASC-N’s Person Identifier (PI) field should not encode the SSN. TIG SCEPACS also specifies PACS interoperability requirements in Section 2.1, 10th paragraph of [4, 2.1]: “For full interoperability of a PACS it must at a minimum be able to distinguish fourteen digits (i.e., a combination of an Agency Code, System Code, and Credential Number) when matching FASC-N based credentials to enrolled card holders.” + The Global Unique Identification number (GUID) field must be present, and shall include a UUID (see Section 3.3), an issuer assigned IPv6 address , or be coded as all zeros (0x00). + The DUNS and Organizational Code fields are optional. + 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 sign the CHUID and the associated certificate shall be placed in the signature field of the CHUID.	SP 800-73-3, Part 1, Section 3.1.2	CHUID
4.3-6	The read access control rule for the X.509 Certificate for PIV Authentication is “Always,” meaning the certificate can be read without access control restrictions.	SP 800-73-3, Part 1, Section 3.1.3	X.509 Certificate for PIV Authentication

Req#	Requirement	Source	Section Title
4.3-7	The Public Key Infrastructure (PKI) cryptographic function (see Table 3) is protected with a "PIN" access rule. In other words, private key operations using the PIV Authentication Key require the Personal Identification Number (PIN) to be submitted, but a successful PIN submission enables multiple private key operations without additional cardholder consent.	SP 800-73-3, Part 1, Section 3.1.3	X.509 Certificate for PIV Authentication
4.3-8	The CBEFF headers shall contain the FASC-N and shall require the Integrity Option.	SP 800-73-3, Part 1, Section 3.1.4	Cardholder Fingerprints
4.3-9	The CBEFF headers shall not require the Confidentiality Option.	SP 800-73-3, Part 1, Section 3.1.4	Cardholder Fingerprints
4.3-10	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 800-73-3, Part 1, Section 3.1.5	Security Object
4.3-11	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 800-73-3, Part 1, Section 3.1.5	Security Object
4.3-12	The card issuer's digital signature key used to sign the CHUID shall also be used to sign the security object.	SP 800-73-3, Part 1, Section 3.1.5	Security Object
4.3-13	The signature field of the security object shall omit the issuer’s certificate, since it is included in the CHUID.	SP 800-73-3, Part 1, Section 3.1.5	Security Object
4.3-14	At a minimum, unsigned data objects, such as the Printed Information data object, shall be included in the Security Object if present.	SP 800-73-3, Part 1, Section 3.1.5	Security Object
4.3-15	The photo on the chip supports human verification only. It is not intended to support facial recognition systems for automated identity verification.	SP 800-73-3, Part 1, Section 3.2.1	Card Holder Facial Image
4.3-16	All FIPS 201 mandatory information printed on the card is duplicated on the chip in this data object.	SP 800-73-3, Part 1, Section 3.2.2	Printed Information
4.3-17	The X.509 Certificate for Digital Signature and its associated private key support the use of digital signatures 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 800-73-3, Part 1, Section 3.2.3	X.509 Certificate for Digital Signature
4.3-18	The X.509 Certificate for Key Management and its associated private key support 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 800-73-3, Part 1, Section 3.2.4	X.509 Certificate for Key Management
4.3-19	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”. If the CAK is implemented, an asymmetric or symmetric CAK is generated by the PIV Card Issuer in accordance with FIPS 140-2 requirements for key generation.A CAK may be generated on-card or off-card. If a CAK is generated off-card, the result of each key generation will be injected into at most one PIV Card.	SP 800-73-3, Part 1, Section 3.2.5	X.509 Certificate for Card Authentication
4.3-20	The Discovery Object, if implemented, is the 0x7E interindustry ISO/IEC 7816-6 template that nests interindustry data objects. For the Discovery Object, the 0x7E template nests two BER-TLV structured interindustry data elements: 1) tag 0x4F contains the AID of the PIV Card Application and 2) tag 0x5F2F lists the PIN Usage Policy.	SP 800-73-3, Part 1, Section 3.2.6	Discovery Object

Req#	Requirement	Source	Section Title
4.3-21	If the first byte of the Tag 0x5F2F (Pin Usage Policy) is set to 0x40, then the second byte is RFU and shall be set to 0x00.	SP 800-73-3, Part 1, Section 3.2.6	Discovery Object
4.3-22	PIV Card Applications that satisfy the PIV ACRs for PIV data object access and command execution with both PIV Card Application PIN and Global PIN shall implement the Discovery Object with the PIN Usage Policy set to 0x60 zz where zz is set to either 0x10 or 0x20.	SP 800-73-3, Part 1, Section 3.2.6	Discovery Object
4.3-23	Up to twenty retired Key Management private keys may be stored in the PIV Card Application. The Key History object provides information about the retired Key Management private keys that are present within the PIV Card Application.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-24	The Key History object shall be present in the PIV Card Application if the PIV Card Application contains any retired Key Management private keys, but may be present even if no such keys are present in the PIV Card Application	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-25	For each retired Key Management private key in the PIV Card Application, the corresponding certificate may either be present within the PIV Card Application or may only be available from an on-line repository.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-26	The Key History object includes two mandatory fields, keysWithOnCardCerts and keysWithOffCardCerts, and one optional field, offCardCertURL.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-27	The offCardCertURL field shall be present if the keysWithOffCardCerts value is greater than zero and shall be absent if the values of both keysWithOnCardCerts and keysWithOffCardCerts are zero.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object

4.3-28	The file that is pointed to by the offCardCertURL field shall contain the DER encoding of the following data structure:
	OffCardKeyHistoryFile ::= SEQUENCE SIZE (1..20) OF SEQUENCE {
	keyReference OCTET STRING (SIZE(1))
	cert Certificate
	}
		SP 800-73-3, Part 1, Section 3.2.7	Key History Object

4.3-29	The private keys for which the corresponding certificates are stored within the PIV Card Application shall be assigned to the lowest numbered key references reserved for retired Key Management private keys. For example if keysWithOnCardCerts is 5, then the corresponding private keys shall be assigned to key references '82', '83', '84', '85', and '86'.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-30	The private keys for which the corresponding certificates are not stored within the PIV Card Application shall be assigned to the highest numbered key references reserved for retired Key Management private keys. For example, if keysWithOffCardCerts is 3, then the corresponding private keys shall be assigned to key references '93', '94', and '95'.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-31	Private keys do not have to be stored within the PIV Card Application in the order of their age. However, if the certificates corresponding to only some of the retired Key Management private keys are available within the PIV Card Application then the certificates that are stored in the PIV Card Application shall be the ones that were most recently issued.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-32	The Key History object is only available over the contact interface. The read access control rule for the Key History object is “Always”, meaning that it can be read without access control restrictions.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-33	The Security Object enforces integrity of the Key History object according to the issuer.	SP 800-73-3, Part 1, Section 3.2.7	Key History Object
4.3-34	These objects hold the X.509 certificates for Key Management corresponding to retired Key Management Keys,	SP 800-73-3, Part 1, Section 3.2.8	Retired X.509 Certificates for Key Management

Req#	Requirement	Source	Section Title
4.3-35	Retired Key Management private keys and their corresponding certificates are only available over the contact interface.	SP 800-73-3, Part 1, Section 3.2.8	Retired X.509 Certificates for Key Management
4.3-36	The read access control rule for these certificates is “Always”, meaning the certificates can be read without access control restrictions.	SP 800-73-3, Part 1, Section 3.2.8	Retired X.509 Certificates for Key Management
4.3-37	The PKI cryptographic function for all of the retired Key Management Keys is protected with a “PIN” access rule. In other words, once the PIN is submitted and verified, subsequent Key Management Key operations can be performed with any of the retired Key Management Keys without requiring the PIN again. This enables multiple private key operations without additional cardholder consent.	SP 800-73-3, Part 1, Section 3.2.8	Retired X.509 Certificates for Key Management
4.3-38	The iris data object specifies compact images of the cardholder’s irises. The images are suitable for use in iris recognition systems for automated identity verification.	SP 800-73-3, Part 1, Section 3.2.9	Cardholder Iris Images
4.3-39	As defined in {"Personal Identity Verification Interoperability For Non-Federal Issuers", IDManagement.gov}, the presence of a Universally Unique IDentifier (UUID) conformant to the specification {IETF RFC 4122, “A Universally Unique IDentifier (UUID) URN Namespace,”} is required in each identification card issued by Non-Federal Issuers, referred to as “PIV Interoperable” (PIV-I) or “PIV Compatible” (PIV-C) cards. The intent of {"Personal Identity Verification Interoperability For Non-Federal Issuers"} is to enable issuers to issue cards that are technically interoperable with Federal PIV Card readers and applications, and that may be trusted for particular purposes through a decision of the relying Federal Department or Agency. Because the goal is interoperability of PIV-I and PIV-C cards with the Federal PIV System, the technical requirements for the inclusion of the UUID are specified ... To include a UUID identifier on a PIV-I, PIV-C, or PIV Card, a credential issuer shall meet the following specifications for all relevant data objects present on an issued identification card. 1. If the card is a PIV-I or PIV-C card, the FASC-N in the CHUID shall have Agency Code equal to 9999, System Code equal to 9999, and Credential Number equal to 999999, indicating that a UUID is the primary credential identifier. In this case, the FASC-N shall be omitted from certificates and CMS-signed data objects. If the card is a PIV Card, the FASC- N in the CHUID shall be populated as described in Section 3.1.2, and the FASC-N shall be included in authentication certificates and CMS-signed data objects as required by FIPS 201. 2. The value of the GUID data element of the CHUID data object shall be a 16-byte binary representation of a valid UUID {IETF RFC 4122}. The UUID should be version 1, 4, or 5, as specified in {IETF RFC 4122}, Section 4.1.3. 3. The same 16-byte binary representation of the UUID value shall be present as the value of an entryUUID attribute, as defined in {IETF RFC 4530, “Lightweight Directory Access Protocol (LDAP) entryUUID Operational Attribute”}, in any CMS-signed data object that is required to contain a pivFASC-N attribute on a PIV Card, i.e., in the fingerprint template and facial image data objects, if present. 4. The string representation of the same UUID value shall be present in the PIV Authentication Certificate and the Card Authentication Certificate, if present, in the subjectAltName extension encoded as a URI, as specified by {IETF RFC 4122}, Section 3. The option specified {by this requirements} supports the use of UUIDs by Non-Federal Issuers. It also allows, but does not require, the use of UUIDs as optional data elements on PIV Cards. PIV Cards must meet all requirements in FIPS 201 whether or not the UUID identifier option is used; in particular, the FASC-N identifier must be present in all PIV data objects as specified by FIPS 201 and its normative references. PIV Cards that include UUIDs must include the UUIDs in all data objects described in (2) through (4).	SP 800-73-3, Part 1, Section 3.3	Inclusion of Universally Unique IDentifiers (UUIDs)

Req#	Requirement	Source	Section Title
4.3-40	Table 1 defines a high level view of the data model. Each on-card storage container is labeled either as Mandatory (M) or Optional (O). This data model is designed to enable and support dual interface cards. Note that access conditions based on the interface mode (contact vs. contactless) take precedence over all Access Rules defined in Table 1, Column 3. Appendix A provides a detailed spreadsheet for the data model. ContainerIDs and Tags within the containers for each data object are defined by this data model in accordance with SP 800-73-3 naming conventions.	SP 800-73-3, Part 1, Section 3.4	Data Object Containers and associated Access Rules and Interface Modes
4.3-41	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 800-73-3, Part 1, Section 4.2	OIDs and Tags of PIV Card Application Data Objects
4.3-42	A data object shall be identified on the PIV client-application programming interface using its OID {as given in Table 2}.	SP 800-73-3, Part 1, Section 4.3	Object Identifiers
4.3-43	An object identifier on the PIV client-application programming interface shall be a dot delimited string of the integer components of the OID [as given in Table 2}.	SP 800-73-3, Part 1, Section 4.3	Object Identifiers
4.3-44	A data object shall be identified on the PIV Card Application card command interface using its BER-TLV tag {using identifiers in Table 2}.	SP 800-73-3, Part 1, Section 4.3	Object Identifiers
4.3-45	A key reference is a one-byte reference data identifier that specifies a cryptographic key or PIN according to its PIV Key Type. Table 3 and SP 800-78, Table 6-1, define the key reference values that shall be used on the PIV interfaces. The key reference values are used, for example, in a cryptographic protocol such as an authentication or a signing protocol. Key references are only assigned to private and secret (symmetric) keys and PINs. All other PIV Card Application key reference values are reserved for future use. When represented as a byte, the key reference occupies bits 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 800-73-3, Part 1, Section 5.1	Key References
4.3-46	The access control rules for PIV data object access shall reference the PIV Card Application PIN and may optionally reference the cardholder Global PIN. If the Global PIN is used by the PIV Card Application, then the Global PIN format shall follow the PIV Card Application PIN format defined in section 2.4.3 of Part 2.	SP 800-73-3, Part 1, Section 5.1	Key References
4.3-47	PIV Card Applications with the discovery object, and the first byte of the PIN Usage Policy value set to 0x60 as per section 3.2.6, shall reference the PIV Card Application PIN as well as the cardholder Global PIN in the access control rules for PIV data object access.	SP 800-73-3, Part 1, Section 5.1	Key References
4.3-48	An algorithm identifier is a one-byte identifier of a cryptographic algorithm. The identifier specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of operation (ECB). SP 800-78, Table 6-2 lists the PIV algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV interfaces.	SP 800-73-3, Part 1, Section 5.2	Algorithm Identifier
4.3-49	The default cryptographic algorithm for the PIV Card Application with algorithm identifier '00' is 3 Key Triple DES – ECB.	SP 800-73-3, Part 1, Section 5.2	Algorithm Identifier
4.3-50	A Status Word (SW) is a 2-byte value returned by a card command at the card edge. The first byte of a status word is referred to as SW1 and the second byte of a status word is referred to as SW2.	SP 800-73-3, Part 1, Section 5.4	Status Words
4.3-51	Recognized values of all SW1-SW2 pairs used as return values on the card command interface and their interpretation are given in Table 5.	SP 800-73-3, Part 1, Section 5.4	Status Words

Req#	Requirement	Source	Section Title
4.3-52	For each container, End-Point compliant cards shall return all TLV elements of the container in the order listed in this appendix.	SP 800-73-3, Part 1, Appendix A	PIV Data Model
4.3-53	Both single-chip/dual-interface and dual-chip implementations are be feasible. In the single-chip/dual-interface configuration, the PIV Card Application shall be provided the information regarding which interface is in use.	SP 800-73-3, Part 1, Appendix A	PIV Data Model
4.3-54	In the dual-chip configuration, a separate PIV Card Application shall be loaded on each chip.	SP 800-73-3, Part 1, Appendix A	PIV Data Model
4.3-55	Note that all data elements of the following data objects are mandatory unless specified as optional.	SP 800-73-3, Part 1, Appendix A	PIV Data Model
4.3-56	Elements of each data object shall be preceded with the assigned tag as noted in Appendix A of SP 800-73.	SP 800-73-3, Part 1, Appendix A	PIV Data Model
4.3-57	Note: The previously deprecated Employee Affiliation Line 2 data element (tag 0x03) has been eliminated, as it did not have a corresponding text field on the face of the card. In order to successfully match the printed information for verification on Zone 8 (Employee Affiliation) and Zone 10 (Organization Affiliation) on the face of the card with the printed information stored electronically on the card, agencies should use tags 0x02, 0x07 and 0x08.	SP 800-73-3, Part 1, Appendix A, Table 13. Printed Information	Printed Information
4.3-58	Recommended length. The certificate that signed the Fingerprint I and II data element in the Cardholder Fingerprint data object can either be stored in the CHUID or in the Fingerprint I and II data element itself. If the latter, the “Max. Bytes” value quoted is a recommendation and the signer certificate in CBEFF_SIGNATURE_BLOCK can exceed the “Max. bytes”.	SP 800-73-3, Part 1, Appendix A, Table 10. Cardholder Fingerprints, Table 12. Cardholder Facial Image	Cardholder Fingerprints, Cardholder Facial Image
4.3-59	The CertInfo byte in the certificate data objects identified above shall be encoded as follows b8 b7 b6 b5 b4 b3 b2 b1 RFU8 RFU7 RFU6 RFU5 RFU4 IsX509 CompressionTypeLsb CompressionTypeMsb	SP 800-73-3, Part 1, Appendix A	PIV Data Model
4.3-60	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 800-73-3, Part 1, Appendix A	PIV Data Model

Req#	Requirement	Source	Section Title

4.3-61	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 800-73-3, Part 1, Appendix A	PIV Data Model

4.3-62	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 Application Identifier (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 800-73-3, Part 2, End-Point PIV Card Application Card Command Interface, Section 2	Overview: End-Point Concepts & Constructs [see Note 1 below]
4.3-63	All PIV Card Application card commands SHALL be supported by a PIV Card Application (Table 2). Card commands indicated with a 'Yes' in the Command Chaining column shall support command chaining for transmitting a data string too long for a single command as defined in ISO/IEC 7816-4 [3]. • PIV Card Application Card Commands for Data Access Commands: SELECT, GET DATA • PIV Card Application Card Commands for Authentication: VERIFY, CHANGE REFERENCE DATA, RESET RETRY COUNTER, GENERAL AUTHENTICATE (chain support required) • PIV Card Application Card Commands for Credential Initialization and Administration: PUT DATA (chaining support required), GENERATE ASYMMETRIC KEY PAIR (chaining support required) 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 2. Note: Cryptographic protocols using private/secret keys requiring “PIN” security condition SHALL not be used on the contactless interface.	SP 800-73-3, Part 2, End-Point PIV Card Application Card Command Interface, Section 3	End-Point PIV Card Application Card Command Interface [see Note 1 below]
4.3-64	SP 800-73-3 Part 3 conformant PIV Middleware shall implement all PIV Middleware functions listed in Table 1 and be able to recognize and process all mandatory and optional PIV data objects.	SP 800-73-3, Part 3, End-Point Client Application Programming Interface, Section 3	End-Point Client Application Programming Interface [see Note 2 below]

NOTES ON SP 800-73-3 REQUIREMENTS

[1]	*NIST Personal Identity Verification Program (NPIVP) product certification testing addresses the PIV Card Application and PIV client application programming interface (API) requirements in SP 800-73-3 Part 2, End-Point PIV Card Application Card Command Interface; the FIPS 201 EP Requirements Traceability Matrix (RTM) therefore only summarizes the Part 2 requirements.*
[2]	*NPIVP product certification testing addresses the PIV Middleware interface requirements in SP 800-73-3 Part 3, End-Point PIV Client Application Programming Interface; the FIPS 201 EP Requirements Traceability Matrix (RTM) therefore only summarizes the Part 3 requirements.*

Req#	Requirement	Source	Section Title
[3]	*The requirements in SP 800-73-3 Part 1, End-Point PIV Card Application Namespace, Data Model and Representation, address the FIPS 201 EP-related requirements for Interfaces for Personal Identity Verification outlined in SP 800-73-3 Part 4, The PIV Transitional Interfaces and Data Model Specification; the EP Requirements Traceability Matrix (RTM) therefore does not directly reference SP 800-73-3 Part 4, to avoid unnecessary duplication of requirements.*		

SP 800-78-3: Cryptographic Algorithms and Key Sizes for PIV

5.1-1	<reserved>	SP 800-78-2	
5.3-2	PIV Cards must implement private key computations for one or more of the algorithms identified in this section (Section 3.1).	SP 800-78-2, Section 2	Application of Cryptography in FIPS 201
5.3-3	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 800-78-2, Section 2	Application of Cryptography in FIPS 201
5.3-4	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 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-5	Note that use of 1024-bit RSA for digital signature and key management keys was phased out in 2008. The use of 1024-bit RSA for authentication keys is permitted to leverage current products and promote efficient adoption of FIPS 201, but must be phased out by 12/31/2013.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-6	Two key Triple-DES (2TDEA) authentication keys must be phased out by 12/31/2010.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-7	In addition to the key sizes, keys must be generated using secure parameters.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-8	Rivest, Shamir, Adleman (RSA) keys must be generated using appropriate exponents, as specified in Table 3-2.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-9	Elliptic curve keys must correspond to one of the following recommended curves from [FIPS186]: + Curve P-256; or + Curve P-384.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-10	To promote interoperability, this specification further limits PIV Authentication and Card Authentication elliptic curve keys to a single curve (P-256). PIV cryptographic keys for digital signatures and key management may use P-256 or P-384, based on application requirements. There is no phase out date specified for either curve.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-11	Implementations of this specification must choose an exponent that is an odd positive integer greater than or equal to 65,537 and less than 2^256, as specified in Table 3-2.	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-12	This specification requires that the Key Management Key must be an RSA key transport key or an Elliptic Curve Diffie-Hellman (ECDH) key. The specifications for RSA key transport are [PKCS1] and [SP800-56B]; the specification for ECDH is [SP800-56A].	SP 800-78-2, Section 3.1	PIV Cryptographic Keys
5.3-13	Table 3-3 provides specific requirements for digitally signed information stored on the PIV Card.	SP 800-78-2, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.3-14	For signatures on the X.509 public key certificates, the CHUID, Security Object, and stored biometrics, the hash algorithm that must be used to generate the signature is determined by the signature generation date.	SP 800-78-2, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.3-15	2010 is a transition period where both SHA-1 and SHA-256 are recommended for generation of RSA signatures. Beginning in 2011, only SHA-256 may be used to generate RSA signatures on PIV objects.	SP 800-78-2, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.3-16	Implementations of this specification [PSS padding scheme] must use the SHA-256 hash algorithm when generating RSA-PSS signatures.	SP 800-78-2, Section 3.2.1	Specification of Digital Signatures on Authentication Information
5.3-17	The object identifiers specified in Table 3-4, below, must be used in FIPS 201 implementations to identify the signature algorithm.	SP 800-78-2, Section 3.2.1	Specification of Digital Signatures on Authentication Information

Req#	Requirement	Source	Section Title
5.3-18	FIPS 201 requires generation and storage of an X.509 certificate to correspond with each asymmetric private key contained on the PIV Card.	SP 800-78-2, Section 3.2.2	Specification of Public Keys In X.509 Certificates
5.3-19	Table 3-5, below, specifies the object identifiers that may be used in certificates to indicate the algorithm for a subject public key.	SP 800-78-2, Section 3.2.2	Specification of Public Keys In X.509 Certificates
5.3-20	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 800-78-2, Section 3.2.2	Specification of Public Keys In X.509 Certificates
5.3-21	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 800-78-2, Section 3.2.3	Specification of Message Digests in the SP 800-73 Security Object
5.3-22	The set of acceptable algorithms depends upon the signature generation date, as specified in Table 3-3.	SP 800-78-2, Section 3.2.3	Specification of Message Digests in the SP 800-73 Security Object
5.3-23	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 800-78-2, Section 3.2.3	Specification of Message Digests in the SP 800-73 Security Object
5.3-24	The CRLs and OCSP status responses are digitally signed to support authentication and integrity using a key size and hash algorithm that satisfy the requirements for signing PIV information, as specified in Table 3-3, and that are at least as large as the key size and hash algorithm used to sign the certificate.	SP 800-78-2, Section 4	Certificate Status Information
5.3-25	CRLs and OCSP status responses that only provide status information for certificates that were signed with 1024- bit RSA keys may be signed using 1024-bit RSA keys. CRLs and OCSP status responses that only provide status information for certificates that were signed with RSA with SHA-1 and PKCS #1 v1.5 padding may be signed using RSA with SHA-1 and PKCS #1 v1.5 padding through 12/31/2013. CRLs and OCSP status responses that provide status information for both certificates that were signed with RSA with SHA-1 and PKCS #1 v1.5 padding and certificates that were signed with other signature algorithms may be signed using RSA with SHA-1 and PKCS #1 v1.5 padding through 12/31/2011.	SP 800-78-2, Section 4	Certificate Status Information
5.3-26	The object identifiers specified in Table 3-4 must be used in CRLs and OCSP messages to identify the signature algorithm.	SP 800-78-2, Section 4	Certificate Status Information
5.3-27	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 800-78-2, Section 5	PIV Card Management Keys
5.3-28	Table 6-1 defines the key reference values used on the PIV interfaces for PIV Key Types.	SP 800-78-2, Section 6.1	Key Reference Values
5.3-29	Table 6-2 lists the algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV interfaces.	SP 800-78-2, Section 6.2	PIV Card Algorithm Identifiers
5.3-30	Table 6-3 summarizes the set of algorithms supported for each key reference value based on the time period of use.	SP 800-78-2, Section 6.3	Algorithm Identifiers for PIV Key Types

SP 800-79-1: Guidelines for the Accreditation of PIV Card Issuers (PCI's)

6.1-2	The organization develops and implements a PCI operations plan according to the template in Appendix D. The operations plan references other documents as needed.	SP 800-79-1, Section 2.11	Accreditation Submission Package and Supporting Documentation
6.1-3	Minimum physical controls at the PCI Facility are implemented. These include: (i) use of locked rooms, safes, and cabinets (as appropriate); (ii) physical access to key areas within the facility is restricted to authorized personnel, (iii) security monitoring and automated alarms are implemented, (iv) emergency power and lighting are available, and (v) fire prevention and protection mechanisms are implemented.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-4	PCI Documentation (e.g., operations plan, standard operating procedures, and contracts) are maintained at each PCI Facility	SP-800-79-1, Appendix G	Commonly accepted security readiness measures

Req#	Requirement	Source	Section Title
6.1-5	The PCIF Manager(s) has a copy of the contingency/disaster recovery plan for the information systems, which is stored securely.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-6	The information systems are managed using a system development life cycle (SDLC) methodology that includes information security considerations.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-7	Enrollment/identity proofing and card activation/issuance workstations are situated in an enclosed area (wall or partition) to provide privacy for an applicant or card holder.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-8	All operators who perform roles within a PCI Facility in the areas of enrollment/ identity proofing or card activation/issuance are allowed access to information systems only when authenticated through a PIV Card.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-9	All operators who perform roles within a PCI Facility in the areas of enrollment/ identity proofing, adjudication and card activation/issuance have undergone training that is specific to their duties prior to being allowed to perform in that function.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-10	All pre-personalized and personalized smart card stock received from card vendors and card production facilities are received only by authorized personnel who ensure that the card stock is stored securely in the PCI Facility.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-11	The organization maintains a current list of designated points of contact and alternate points of contact for all PCIFs used by the organization for enrollment/identity proofing and card activation/issuance.	SP-800-79-1, Appendix G	Commonly accepted security readiness measures
6.1-12	The organization has completed a lifecycle walkthrough at one year intervals since the last accreditation date, and the results are documented in a report to the DAA.	SP 800-79-1, Section 5.4	Monitoring Phase

SP 800-96: PIV Card to Reader Interoperability Guidelines

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

Req#	Requirement	Source	Section Title
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
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

SP 800-104: A Scheme for PIV Visual Card Topography

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

Req#	Requirement	Source	Section Title
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
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}	SP 800-104, Section 2.4	Color Representation
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

SP 800-116: A Recommendation for the Use of PIV Credentials in PACS

Req#	Requirement	Source	Section Title
9-1	PIV authentication mechanisms should be implemented in accordance with Table 1-1. Figure 1-1 illustrates the innermost perimeter at which each PIV authentication mechanism may be used based on the authentication assurance level of the mechanism. The combined effect of Table 1-1 and Figure 1-1 determines exactly what mechanisms may be used. (See Section 7.3) An exhaustive list of possible uses of PIV authentication mechanisms against protected areas is provided in Appendix C.	SP 800-116, Section 1	Selecting PIV Authentication Mechanism
9-2	A risk-based migration strategy should be planned and implemented to achieve PIV enabling.	SP 800-116, Section 1	Selecting PIV Authentication Mechanism
9-3	Section 508 should be considered early during projects that integrate the PIV System with PACS. Section 508 should be considered as it applies to enrollment software, smart card and biometric readers, monitoring systems, and access control point sensors and actuators.	SP 800-116, Section 2.2	Section 508
9-4	It is recommended that path validation of a PIV authentication certificate be done at PIV registration, and periodically repeated by the PACS server as long as registration is maintained. Implementation methods are further discussed in Sections 7.4 and 7.5.	SP 800-116, Section 4.2	Terminated PIV Cards
9-5	Given the ready availability of high-quality scanners, graphic editing software, card stock, and smart card printers, electronic verification is strongly recommended, either in place of the VIS authentication mechanism or in combination with it.	SP 800-116, Section 4.3	Visual Counterfeiting
9-6	It is strongly recommended that agencies use PKI or asymmetric CAK challenge/response methods instead of the CHUID authentication mechanism (see the Recommendation in Section 4.9).	SP 800-116, Section 4.7	Electric Cloning
9-7	Moreover, since many CHUIDs may be presented while an attacker probes for a valid CHUID, the PACS should employ methods to detect, alarm, and block repeated unsuccessful CHUID presentations.	SP 800-116, Section 4.8	Electric Counterfeiting
9-8	NIST therefore recommends that the CHUID authentication mechanism be implemented in only two situations: 1) access control points separating two areas at the same impact level, either Controlled or Limited; and 2) combined with the VIS authentication mechanism at access points between Unrestricted and Controlled areas. See Section 7 for further detail. NIST further recommends that the asymmetric CAK authentication mechanism be used instead of the CHUID authentication mechanism to the greatest extent practical.	SP 800-116, Section 4.9	Other Threats
9-9	To attain full interoperability, a relying PACS application will need to support all acceptable algorithms, key lengths, and key material that could be presented, either by a PIV Card or by the PIV infrastructure.	SP 800-116, Section 6.1	Interoperability
9-10	The interoperability goal of the PIV-enabled PACS can be stated: 1. Any PIV Card can provide proof of identity to any electronic PACS (access is granted only if the identity is so authorized). 2. After a successful authentication, the authentication mechanism provides the cardholder's authenticated identity, in the form of a FASC-N Identifier (a subset of FASC-N as defined in Section 3), to the relying party.	SP 800-116, Section 6.1	Interoperability
9-11	If the PKI authentication mechanism is performed by a PACS application, the PACS should support all of the asymmetric algorithms permitted for the PIV Authentication Key, as specified in Table 3-1 of [SP800-78], i.e., RSA 1024 (through 31 December 2013), RSA 2048, and ECDSA P-256, and the PACS should accept all valid PIV authentication certificates and require PIN entry.	SP 800-116, Section 6.1	Interoperability
9-12	If the CAK authentication mechanism is performed by the PACS, the accepted algorithms will be the same, but the PACS will accept only Card Authentication Key certificates and not require PIN entry.	SP 800-116, Section 6.1	Interoperability
9-13	If CHUID authentication with signature verification is performed, the PACS should support all of the signature algorithms and key sizes permitted by Table 3-3 of [SP800-78]. If only CHUID authentication without signature verification of the CHUID is performed, no cryptographic operations are performed, and no cryptographic requirement is placed on the PACS.	SP 800-116, Section 6.1	Interoperability
9-14	PINs required for PIV authentication mechanisms are strings of eight or fewer decimal digits. For PKI, BIO, and BIO-A authentication mechanisms, a PIN entry device must acquire PINs from the cardholder and present them to the PIV Card to activate the card.	SP 800-116, Section 6.1	Interoperability

Req#	Requirement	Source	Section Title
9-15	Recommendation: To obtain the full benefit of PIV interoperability, HSPD-12 project managers should ensure that relying systems have the capability to use all cryptographic algorithms that apply to the authentication mechanism(s) performed. Departments and agencies should procure and deploy HSPD-12 products on the GSA HSPD-12 Evaluation Program Approved Products List where applicable, and can use the PIMM presented in Section 9 to measure progress toward the goal of interoperability. [FIPS 201 Evaluation Program]	SP 800-116, Section 6.1	Interoperability
9-16	The PIV System implementation will be complete when the following qualities have been achieved. 1. PIV authentication mechanisms are used wherever they are applicable, in accordance with HSPD-12 and FIPS 201. 2. Electronic authentication (as opposed to VIS authentication) is the common practice. 3. Electronic validation of the PIV Card is done at or near the time of authentication. 4. All PIV Card access control decisions are made by comparing an initial string of the FASC-N Identifier against the ACL entries. See Appendix B for details and examples. 5. PIV authentication mechanisms are applied based on the impact assessed for the area. 6. Cryptographic and biometric authentications are applied widely in moderate- and high-impact [FIPS199] areas. 7. Agencies exhibit reciprocal trust in the process assurance of PCIs. 8. Both new and upgraded PACS applications accept PIV Cards as proof of identity for user registration/provisioning, user authentication, or both.	SP 800-116, Section 6.2	Qualities of Complete Installation
9-17	Recommendation: Once all appropriate authentication mechanisms are satisfied, access control decisions are made by comparing the 14 decimal digit FASC-N Identifier, and optionally the values of additional FASC-N fields, against the ACL entries.	SP 800-116, Section 6.2	Qualities of Complete Installation
9-18	Recommendation: As agencies develop risk-based implementation plans, they will create and evolve plans for PIV Card issuance and application integration. They might consider which of the eight qualities are most relevant to agency goals and priorities, and derive further project objectives, metrics, and milestones from those qualities. They should also consider the relation of HSPD-12 to FISMA requirements, and examine the potential for cost tradeoffs where PIV can replace more expensive authentication methods.	SP 800-116, Section 6.2	Qualities of Complete Installation
9-19	Recommendation: Operational metrics should be designed to measure actual benefits over the operational lifetime of the PIV System. They may be derived by formulating each of the expected benefits above as a service quality metric, e.g., for “integrated system”, service quality could be defined as the percentage of PACS registrations that are performed automatically by provisioning from the PIV issuance system.	SP 800-116, Section 6.3	Benefits of Complete Installation
9-20	Recommendation: Maximum benefit will be obtained from the PIV System when it is adequately supported by infrastructure. Infrastructure upgrades may be justified, especially to improve communication among PACS system elements (e.g., support two-way communication).	SP 800-116, Section 6.4	Infrastructure Requirements
9-21	Reading the CHUID from a PIV Card is not sufficient to establish confidence in cardholder’s identity. Therefore, in order to achieve single-factor authentication with CHUID, the relying parties must validate the signature on the CHUID.	SP 800-116, Section 7.1.3	Cardholder Unique Identifier (CHUID) Authentication
9-22	Recommendation: NIST strongly recommends that every PIV Card contain an asymmetric CAK and corresponding certificate, and that PACS use an asymmetric challenge/response CAK protocol.	SP 800-116, Section 7.1.4	Card Authentication Key (CAK) Authentication
9-23	PACS may be designed to perform public key cryptography-based authentication using the PIV Authentication Key.	SP 800-116, Section 7.1.5	PIV Authentication Key (PKI) Authentication

Req#	Requirement	Source	Section Title
9-24	PACS may be designed to perform biometric authentication using the fingerprint information stored on the PIV Card.	SP 800-116, Section 7.1.6	BIO Authentication
9-25	Recommendation: A PACS should always verify the digital signature on the biometric template data object, and do path validation, before performing a match. Otherwise, the result of the match should not be trusted.	SP 800-116, Section 7.1.6	BIO Authentication
9-26	Recommendation: Biometric readers, especially those used at access points to Limited and Exclusion areas, should have a proven capability to accept live fingers and reject artificial fingers. Biometric readers, especially unattended readers in an Unrestricted area, should be physically hardened to protect against direct electrical compromise.	SP 800-116, Section 7.1.6	BIO Authentication
9-27	an agency may use a Facility Security Level (FSL) Determination to derive the FSL for its facilities.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-28	For these reasons, it is recommended that authentication mechanisms be selected on the basis of protective areas established around assets or resources. This document adopts the concept of “Controlled, Limited, Exclusion” areas as defined in [PHYSEC].	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-29	Access to Exclusion areas may be gained by individual authorization only.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-30	This document recommends that Table 7-2 be used to determine the minimum number of authentication factors needed to satisfy security requirements of the area. Table 7-2. Authentication Factors for Security Areas Security Areas Number of Authentication Factors Required Controlled 1 Limited 2 Exclusion 3	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-31	Authentication mechanisms shown at a perimeter in Figure 7-1 may also be used alone at a perimeter farther out, subject to the requirements in Table 7-2, but not the reverse.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-32	If authentication mechanisms are combined in ways not shown in Figure 7-1, at least one of the combined mechanisms must be allowed by Figure 7-1 at the perimeter of use.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-33	In a particular facility, a single perimeter may separate areas with a difference of more than one impact level. A single perimeter may allow access from Unrestricted to Limited, Unrestricted to Exclusion, or Controlled to Exclusion areas, and in these cases, the PIV authentication mechanisms should be combined to achieve necessary authentication factors to enter the innermost area.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-34	Within a Controlled or Limited area, an access point to an adjacent area at the same impact level may employ any of the authentication mechanisms shown in Figure 7-1, as well as the CHUID authentication mechanism without VIS.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-35	Within an Exclusion area, an access point to an adjacent area at the same impact level should use two or three-factor authentication.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-36	At Threat Conditions Green, Blue, and Yellow, the facility should use the authentication mechanisms at each perimeter as shown. At Threat Condition Orange, the facility should use two or three-factor authentication at the Controlled perimeters.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-37	When the Threat Condition level increases, some access points may be closed. Access points that remain open should be capable of the required authentication mechanisms at the elevated Threat Condition level.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-38	CAK, CHUID + VIS, or BIO authentication mechanisms provide one-factor authentication and can be used to cross from Uncontrolled to Controlled areas.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-39	BIO-A or PKI authentication mechanisms provide two-factor authentication and can be used to cross into Limited areas.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms

Req#	Requirement	Source	Section Title
9-40	Recommendation: Authentication assurance will be increased if a PACS uses relevant information from previous access control decisions ("context") when making a new access control decision. For example, if a cardholder attempts to pass from a Controlled to a Limited area, the PACS could require that the cardholder was recently allowed access to the Controlled area. Historically, rigorous implementation of this concept required person-traps and exit tracking, but partial implementations have significant value, and could be strengthened by new technology and systems integration.	SP 800-116, Section 7.3	Selection of PIV Authentication Mechanisms
9-41	Before a PACS may grant access to a cardholder, the cardholder must be authorized for access in the PACS.	SP 800-116, Section 7.4	PACS Registration
9-42	Authorization may be granted to a group of individuals, such as all PIV cardholders, or all PIV cardholders sponsored by a specific agency or bureau (see Appendix B). If authorization is granted to specific individuals, information about the cardholder (specifically, at least the FASC-N) must be added to the PACS Server's authorization database.	SP 800-116, Section 7.4	PACS Registration
9-43	If a caching status proxy is employed, information about the cardholder, including the cardholder's certificate, must be added to the server's database.	SP 800-116, Section 7.4	PACS Registration
9-44	Where one-factor authentication is sufficient, the CAK or PKI certificate may be used. Where at least two-factor authentication is required, the PIV Authentication Key certificate should be used.	SP 800-116, Section 7.4	PACS Registration
9-45	Enrollment using a caching status proxy should collect and store information required for all FIPS 201 authentication mechanisms needed in the event of increased Threat Condition level.	SP 800-116, Section 7.4	PACS Registration
9-46	Recommendation: When a card is terminated, the PIV Card Issuer must revoke all valid authentication certificates for the PIV Card. The authentication certificates include the PIV Authentication Key certificate and the Card Authentication Key certificate (if present).	SP 800-116, Section 7.4	PACS Registration
9-47	Since certificate revocation is used as a mechanism to indicate that a PIV Card should no longer be considered valid, the caching status proxy should periodically re-validate all of the certificates in its database and deactivate the access privileges of any individual whose certificate has expired or has been revoked.A40	SP 800-116, Section 7.4	PACS Registration
9-48	Re-validation should be performed by the caching status proxy at least once per day. Once the decision has been made to revoke a PIN credential, agencies may employ local de-authorization methods to supplement revocation and achieve a more rapid local effect.	SP 800-116, Section 7.4	PACS Registration
9-49	Recommendation: The CHUID may be collected at registration, but it should be treated as if it were a password (since digital signature provides entropy equivalent to a password) for purposes of retention, i.e., hashed, the hash stored, and the CHUID deleted. A stored CHUID presents risks similar to a stored password; it can be copied and used to gain access. Data elements may be extracted from the CHUID and retained (e.g., the FASC-N, Data Universal Numbering System (DUNS) Number, and Global Unique Identifier (GUID)), and a retained hash is sufficient to enable verification. NIST strongly recommends against the storage of complete CHUIDs in relying systems.	SP 800-116, Section 7.4	PACS Registration
9-50	Recommendation: PKI and asymmetric CAK authentication mechanisms should be implemented by a PACS reader capable of full certificate path validation, either on-line or using a caching status proxy. Agencies should consider using on-line status checks as a means to reduce the latency of PIV Card status when a PIV Card is used for access to Exclusion areas. If a caching status proxy is used, the certificates should be captured when the PIV Card is registered to the PACS.	SP 800-116, Section 7.4	PACS Registration
9-51	The cache status should be updated at least once every 24 hours.	SP 800-116, Section 7.5	Credential Validation and Path Validation
9-52	Recommendation: On-line credential validation should be implemented for all of the FIPS 201 authentication mechanisms whenever possible. It is especially important when the one-factor, non-biometric mechanisms (CHUID, CAK) are used, because they could be exploited by simple possession of a misappropriated PIV Card. Caching techniques can be used to implement credential validation when on-line, on-demand credential validation is not possible. It is also recommended that the cached data be protected against tampering.	SP 800-116, Section 7.5	Credential Validation and Path Validation
9-53	Data objects read from a smart card by a reader should not be fully trusted as authentic (i.e., produced by a PCI) and unmodified until their digital signatures are verified.	SP 800-116, Section 7.5	Credential Validation and Path Validation

Req#	Requirement	Source	Section Title
9-54	Recommendation: Path validation should be performed on all signed data objects required by the authentication mechanism in use. Path validation should employ on-line credential validation where possible, or cached certificate status where on-line certificate validation is not possible.	SP 800-116, Section 7.5	Credential Validation and Path Validation
9-55	Recommendation: Because having on-card role and permission information would raise difficult challenges concerning update and revocation, PACS permissions should generally be stored in a PACS facilities-based component, such as a panel or controller database.	SP 800-116, Section 8.6	Role-Based Access Control
9-56	Agencies should apply appropriate (in accordance with Table 7-2) PIV authentication mechanisms to the areas to ensure that incident management personnel, emergency response providers, and other personnel (including temporary personnel) and resources likely needed to respond to a natural disaster, act of terrorism, or other manmade disaster can be electronically authenticated in order to attain movement internal to Federally controlled facilities and areas within the incident scene.	SP 800-116, Section 8.8	Disaster Response and Recovery Incidents
9-57	PACS application providers should only employ products that are approved through the FIPS 201 evaluation program where the evaluation program product categories are applicable. [FIPS 201 Evaluation Program]	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-58	For each access transaction, once the applicable authentication mechanisms are satisfied, all PACS access decisions are based on utilization of the complete FASC-N Identifier (match of the 14 digit Agency Code, System Code, and Credential Number) which is unique across Federal government agencies.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-59	The PACS application that uses PKI or asymmetric CAK authentication mechanisms should support all of the asymmetric algorithms specified in Table 3-1 of [SP800-78].	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-60	Each facility should be mapped to the “Controlled, Limited, Exclusion” model and an assignment of PIV authentication mechanisms to all access control points in accordance with Section 7.1.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-61	Signature verification and path validation should be performed on all signed data objects in the PIV authentication mechanisms used.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-62	On-line credential validation should be implemented for all authentication mechanisms whenever connectivity is available. Caching techniques may be used to reduce connectivity requirements.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-63	The CHUID authentication mechanism should be implemented in only two situations: 1) access control points separating two areas at the same impact level, either Controlled or Limited; and 2) combined with the VIS authentication mechanism at access points between Unrestricted and Controlled areas. See Section 4.9.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-64	The CHUID data object may be read from the PIV Card and used for registration and authentication transactions, but should not be retained in a PACS or other relying system after the transaction is complete. If the values of the CHUID data fields must be retained, the asymmetric signature of the CHUID should be deleted.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-65	All PACS applications should operate at PIMM Level 5.	SP 800-116, Section 9.7	PIV-in-PACS Best Practices
9-66	Recommendation: Agencies should collaborate to standardize an enhancement or replacement of the FASC-N that accomplishes both credential identification and object binding, and supports an extensible framework for subject identification.	SP 800-116, Section 10.1	Generalized Credential Identifier
9-67	Recommendation: SBMOC should be pursued as a standard FIPS 201 authentication mechanism, especially for PACS. Assuming it is judged to be at least as trustworthy as PIN entry, SBMOC should be allowed to substitute for PIN to activate a PIV Card.	SP 800-116, Section 10.2	Secure Biometric Match on Card