Document Guide

1. This document extracts and consolidates policy statements and high level technical requirements that impact policy from FIPS PUB 201 PUBLIC DRAFT
2. Each is consecutively numbered
3. Where ever possible, policy and requirements have been recast from free text into tables – for clarity, concision, and to help highlight omissions
4. The FIPS 201 outline is preserved and followed
5. *The author's comments, observations, and opinions are specified in italics*

2 Common Identification and Security Requirements

2.1 Control Objectives

A. Use Government-wide identity proofing and registration processes defined in Section 2.2
B. Use Government-wide identity credential issuance processes defined in Section 2.3
C. Issue credentials through systems and providers whose reliability has been established by the agency and so documented and approved in writing
D. Issue identity credentials that are resistant to identity fraud, tampering, counterfeiting, and terrorist exploitation
E. Implement an identity credentialing system that supports rapid electronic authentication of Federal employees and contractors
F. Support credentials for physical and logical access to Federally controlled facilities and information systems

2.2 Identity Proofing and Registration Process

1. Five *critical* roles associated with PIV identity proofing and issuance.
   - Applicant (A)
   - Requesting Official (RO)
   - Authorizing Official (AO)
   - Registration Authority (RA) (performs identity proofing and background checks)
   - Issuing Authority (IA)
2. Individuals shall not assume more than one role

2.2.1 Identity Proofing and Registration of New Employees and Contractors

3. Applicant provides two I-9 forms of ID to ~~RA~~ RO
4. At least one is a valid State or Federal Government-issued picture ID
   - *Unanswered Question – how does someone get their 1st government-issued picture ID*
5. *[Implied] A PIV request is begun (paper or eForm)*
6. RO submits PIV Request, with photocopies of source docs, to AO
7. AO approves request and forwards with source docs to both RA and IA
8. PIV request includes:

Information Required for a PIV Request	***Applicant***	***Requesting Official***	***Authorizing Official***	***Registration Authority***	***Issuing Authority***

Name	Yes	Yes	Yes	Yes	Yes
Organization	?	Yes	Yes	-	-
Contact Info	Yes	Yes	Yes	Yes	Yes
Address of parent organization	Yes				
Date of Birth	Yes				
Position	Yes	-	-	-	-
Position Sensitivity Level	Yes	-	-	-	-
Signature	-	Yes	Yes	-	-

9. There are four (*seems like five*) position sensitivity levels:
   - 1. Low
   - 2. Moderate
   - 3. High
   - 4a. Critical - Vital National Asset-Critical Infrastructure
   - 4b. Critical - High Risk Public Trust Position

10. Background information forms are required, vary by sensitivity level:

Background Information Forms Required	1. Low	2. Moderate	3. High	4a. Critical	4b. High Risk
• Form I-9, OMB No. 1115-0136, Employment Eligibility Verification	Yes	-	-	-	-
• Standard Form 85, OPM Questionnaire for Non-Sensitive Positions or equivalent	-	Yes	-	-	-
• Standard Form 85 P, OPM Questionnaire for Public Trust Positions or equivalent	-	-	Yes	Yes	Yes

11. Applicant provides completed background information form to RA
12. Applicant provides same two I-9 source documents to RA
13. RA visually inspects and authenticates source documents
14. RA visually compares picture ID with Applicant to confirm identity
15. RA compares info on source documents with info provided in PIV request
16. RA collects fingerprints from applicant
17. RA performs background checks, which vary by positions sensitivity,:

Background Checks	1. Low	2. Moderate	3. High	4a. Critical	4b. High Risk
1. Identity Source Documents Check (verified with issuer)	Yes	Yes	Yes	Yes	Yes
2. Law Enforcement Check (fingerprint)	Yes	Yes	Yes	Yes	Yes
3. National Agency Check (NAC).					
• Security/Suitability Investigation Index (SII)	-	Yes	Yes	Yes	Yes
• Defense Clearance Investigation Index (DCII)	-	Yes	Yes	Yes	Yes
• FBI Name Check	-	Yes	Yes	Yes	Yes
• FBI National Criminal History Fingerprint Check	-	Yes	Yes	Yes	Yes
4. NAC with written Inquiries (NACI)					
• Employment	-	5 yrs	5 yrs	3 yrs	5 yrs
• Education, with highest degree verified	-	5 yrs	5 yrs	3 yrs	5 yrs
• Residence	-	3 yrs	3 yrs	1 yr	5 yrs
• References	-	Yes	Yes	1 yr	-
• Law Enforcement	-	5 yrs	5 yrs	5 yrs	5 yrs
4. NACI with Credit Record Search (NACIC)					
• Credit	-	-	?	7 yrs	7 yrs
5. Limited Background (LBI) & Background Investigations (BI)					
• PRSI Personal Subject Interview (PRSI)	-	-	-	Yes	Yes
• Court Records	-	-	-	3 yrs	?

18. Upon successful completion of background check, RA notifies IA credential can be issued
    - *What action is taken on unsuccessful background check?*
    - *Regardless of trustworthiness, if the identity has been proven, a PIV must still be issued?*

19. The RA maintains
    - Completed and signed PIV
    - Copies of identity source documents
    - Completed and signed background form
    - Results from background check
    - Any other materials used to prove the identity of the applicant

2.2.2 Identity Proofing and Registration of Current Employees

20. Same process as in 2.2.1 with one exception - Background checks are not required if most recent check is on file and RA can verify

2.2.3 Access Pending Identity Proofing

21. Applicants shall be treated according to visitor procedures until background checks complete

2.2.4 Identity Proofing and Registration of Overseas Foreign Workers

22. Dept. of State Bureau of Diplomatic Security will approve a similar process for registration and approval for foreigners working for the US Federal Government overseas

2.3 Identity Credential Issuance

23. IA validates PIV requests received from AO notification received from RA
    - *Specific validation requirement is not specified, presumably one of telephone call, fax, visual inspection of paper copy, digital signature of electronic copy, …)*
24. Applicant appears in person to IA and presents source documents
25. IA verifies that the individual that who collects the identity credential is indeed the applicant, by matching presented source documents to photocopies taken at time of application
26. IA photographs Applicant at time of issuance and retains a file copy of image
27. The PIV card is personalized for the Applicant

These last two statements mandate decentralized, on-site personalization (electrical and graphical) as is currently performed with the DoD CAC. It specifically disallows centralized personalization as is currently performed with passports and the TWIC. Should be reversed. Centralized issuance should absolutely be left as an option. It has many desirable properties, including economies of scale, tighter controls, and stronger assurance that the system has not been circumvented.

28. IA maintains:
    - Completed and formally authorized PIV request
    - Name of Applicant (seems to be redundant with previous bullet)
    - Credential Identifier *("such as" is too vague. Need to be specific for uniformity)*
    - Expiration Date

There is no policy regarding forward of information to central PIV registry. This would be needed if, for instance, a check for duplicate PIV cards issued to the same individual is made via a one-to-many biometric check.

3 PIV System Overview

Informative, not normative. Does not levy any requirements or policy

4 Front-End System

4.1 PIV Card Specifications

29. PIV card physical characteristics shall comply with established standards: ISO/IEC 7810, ISO/IEC 10373, ISO/IEC 7816, ISO/IEC 1443.

4.1.1 Printed Material

Does not levy any policy or high level requirement. May be more of a requirement for the printing equipment and ink than the card.

4.1.2 Physical Security Tamper Proofing and Resistance

30. The PIV card shall include an optical variable device (OVD)
31. The PIV card may include additional tamper resistance and anti-counterfeiting methods.

There is no policy regarding uniform appearance of graphical security features that would allow a moderately trained individual to detect tampered or counterfeited PIVs. Just as with other items of value that must be protected from counterfeiting (e.g. currency and passports), the graphical security features on PIVs must be uniform so that a moderately trained individual can detect a fake or tampered PIV.

4.1.3 Physical Characteristics and Durability

32. The card shall contain a contact and contactless ICC interface
33. The card shall not be embossed, punched, or affixed with decals.

The actual construction of the card, its tolerance for water and mild soap, tolerance for sunlight, and other durability specifics are more appropriate for agency specific procurement documents. These statements should not be codified within FIPS 201 as policy applying across the entire government.

4.1.4 Topography [Graphical Layout] Requirements

34. The PIV card shall conform to a common format on the front of the card, and one of two standard formats for the reverse. The zones are enumerated below:

Note that the location (horizontal and vertical offsets) and size (width and height) should be completely specified in FIPS 201. These have not been specified.

Note: Zone numbering should be such that zone numbers are unique. (e.g. front 1-14, reverse 20-29, military reverse 31-39)

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

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

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

The information and diagrams provided in FIPS 201 are not sufficient to assure uniformity in appearance of PIV cards issued throughout the Federal Government. Also, the flexibility of issuers to choose font sizes above the minimum reduces the degree to which all credentials will have a uniform appearance. Where possible and reasonable, font sizes should be specified, not just the minimum.

Four different fonts have been specified:

Font	Zones
Arial Bold Black	f8, f9
Arial Bold	f2, r1, r2
Arial Black	f10, f11(?), f13, f14, r5
Arial	r4, r6, r7, r8
Unspecified	f4, f5, f12

Zn	Field	Description	Sample
f2	Name	Arial Bold, all caps, ≥ 10 pt Surname above, First name below	**SURNAME** **FIRSTNAME**
f8	Affiliation	Arial Bold Black, all caps, ≥ 7 pt	**CONTRACTOR**
f9	US Government	Arial Bold Black, all caps, ≥ 7 pt	**UNITED STATES GOVERNMENT**
f14	Expiration Date	"Expires", Arial Black, ≥ 6 pt, "YYYY/MM", Arial Black, ≥10 pt	**Expires** **2008/06**
r1	Agency CSN	Arial Bold, ≥10 pt, Format at discretion of Issuer	**USANIST0101842**
r2	Issuer Id Number	Arial Bold, ≥10 pt, Department Code (6 characters) + Agency Code (4 characters) + Issuing Agency (5 digits)	**USADOCNIST00001**
f4	Pay Grade	Format at discretion of Issuer	*Unspecified*
f5	Rank	Format at discretion of Issuer	*Unspecified*
f10	Agency Name	Arial Black. ≥ 7 pt	**US Agency Agency**
f11	Agency Seal	Arial Black. ≥ 7 pt (?)	*This is a picture, not print*
f12	Emergency Response	Font ???. Size ??? "Federal Emergency Response Official"	*Unspecified*
f13	Issue Date	"Issued", Arial Black, ≥ 6 pt, "YYYY/MM", Arial Black, ≥10 pt	**Issued** **2008/06**
r4	Return To	Return Address - Arial. ≥ 6 pt	Return to: Security Manager's Office (CAPS) 1800 F Street, N.W. Washington, DC 20405
r5	Physical Characteristics	Arial Black. ≥ 7 pt e.g. height, eye color, hair color	**Height** **5'11"** **Eyes:** **Brown** **Hair:** **Brown**
r6	ER Language	Arial. ≥ 5 pt "The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas."	The bearer of this card is a designated Emergency Responder. After credential verification, bearer should be given access to controlled areas.
r7	Title 18 Lang.	Arial. ≥ 6 pt	This credential is the property of the United States Government. Counterfeiting, altering, or misusing violates Section 499, Title 18 of the U.S. Code.
r8	Lost Card	Instructions – Arial. ≥ 6 pt	Drop in any post office box for return.

35. The following personal information shall be included graphically on the surface of the on the card:
    - Photo
    - Name
    - Medical (military only, per Geneva Convention)
    - Date of Birth (military only, per Geneva Convention)
    - Social Security Number (military only, per Geneva Convention)

36. At the issuer's option, the following personal information may be included graphically on the surface of the on the card:
    - Signature
    - Pay Grade
    - Rank
    - Physical characteristics (non-military only, height, hair color, eye color, …)
      Note: an exhaustive list of what is permitted should be enumerated.

37. [Implied] No other personal information may be included graphically on the surface

Note: there is no policy statement for what personal information may and may not be included in the optional bar codes and magnetic stripe. An exhaustive list of what is permitted for each should be enumerated.

4.1.5 Logical Credentials

4.1.5.1 Logical Credential Data Model

38. The PIV card shall include the following data electrically in the ICC:
    - Personal Identification Number (PIN)
    - Cardholder Unique Identifier (CHUID) object
    - A public/private key pair and certificate for authentication
    - Two fingerprint images
    - Facial image

39. The PIV card may additionally include the following data electrically in the ICC:
    - A public/private key pair and certificate for digital signature
    - A public/private key pair and certificate for key management
    - Additional public/private key pairs and certificates for local physical access
    - Additional secret keys for local physical access
    - Secret key(s) associated with the card management system

40. The credentials on the card may be used for 3 kinds of cardholder authentication – to card, to external entity, and to CMS – as follows:

	Form of Authentication		
Credential	**Cardholder to Card**	**Cardholder to External Entity**	**CMS to Card**
PIN	Yes	-	-
Fingerprints	With Match on Card	Yes	-
Facial Image	With Match on Card	Yes	-
CHUID	-	Yes	-
Authentication PK	-	Yes	-
Digital Signature PK	-	Yes	-
Key Management PK	-	Yes	-
Physical Access PK	-	Yes	-
Physical Access SK	-	Yes	-
CMS Secret Key	-	-	Yes

This is slightly oversimplified, because the entity performing the authentication is not shown. This is remedied as follows:

		Form of Authentication					
	Authentication by:	PIV Card			External Entity		CMS
	Authentication of:	CH	External	CMS	CH	PIV	PIV
Kind	**Credential**						
User Info	PIN	MOC	-	-	MEC	-	-
User Bio	Fingerprints	MOC	-	-	MEC	-	-
	Facial Image	MOC	-	-	MEC	-	-
Public Key Crypto	CHUID	-	-	-	-	Yes	-
	Authentication PK	-	-	-	-	Yes	-
	Digital Signature PK	-	Yes	-	-	Yes	-
	Key Management PK	-	Yes	-	-	Yes	-
	Physical Access PK	-	Yes	-	-	Yes	-
Secret Key Crypto	Physical Access SK	-	C/R	-	-	C/R	-
	CMS Secret Key	-	-	C/R	-	-	C/R

CH = Cardholder,	**MOC** = Match on Card	**MEC** = Match External to Card
PK = Public Key	**SK** = Secret Key	**C/R** = Challenge/Response

4.1.5.2 File Structure

41. The CHUID and biometric information shall be stored as transparent files in the Master File

4.1.6 PIV Card Activation

42. The PIV must be activated to perform privileged operations. Activation may occur in one of two ways:
    - Authentication the cardholder (e.g. by PIN code or biometric)
    - Authenticating the CMS

4.1.6.1 Activation by Cardholder

43. Every PIV card shall implement PIN-based cardholder activation
44. PIV cards may optionally implement biometric-based activation
45. PIN shall be numeric
46. PIV card shall include mechanisms to limit number of PIN guesses
47. PIN authentication shall meet FIPS 140-2 Level 3 for Operator Authentication
    - PIN code shall be at least 6 digits in length
    - PIN code shall not be transmitted to the card in clear text

Note: the FIPS 140-2 Level 3 requirement to NOT transmit the PIN in clear text requires some form of scrambling (e.g. encrypted with shared symmetric key, challenge/response followed by hashed PIN, challenge/response followed by digital signed PIN). It is critical that the federal Government select a single mechanism and use it uniformly throughout all government applications. Otherwise, cards will NOT generally be interoperable at PIN pad locations.

48. Biometric-based card activation may only be used if the biometric match is performed on the PIV card (MOC).
49. Biometric-based card activation, the choice of biometrics, the algorithms and techniques are all local issuer decisions.

4.1.6.2 Activation by Card Management System

50. At the issuer's option, PIV cards may support activation by CMS
51. To activate the card, the CMS shall perform a challenge response using cryptographic keys stored on the card
52. At time personalization, CMS keys shall be set to values specific to each card. (That is, a card issuer may not use a single cryptographic key to activate more than one card.)
53. Card management system keys are permitted as follows:

Algorithm	First permitted issue date	Last permitted expiration date
Two Key Triple-DES (TDEA2)	1/1/2005	12/31/2010
Three Key Triple DES (TDEA3)	1/1/2005	?
AES-128	1/1/2005	?
AES-192	1/1/2005	?
AES-256	1/1/2005	?

An important and unaddressed interoperability/change management issue is the policy/mechanism regarding how the card and reader determine the cryptographic algorithms available and negotiate which will be used. Possibilities include:

- *Card dictates (so the reader must supports all algorithms)*
- *Card presents list of algorithms available, reader selects*
- *Reader presents list of algorithms available, card selects*

4.2 Cardholder Unique Identifier (CHUID)

54. The PIV shall contain an elementary file for the CHUID
55. The PIV CHUID shall be digitally signed by the IA
56. The CHUID shall be accessible from both the contact and contactless interfaces
57. The CHUID shall be accessible without activation (e.g. without PIN or biometric)
58. The PIV FASC-N shall not be modified post issuance
    - *ACRs are applied at the generic container level (i.e. the CHUID) For the card to enforce this policy, the CHUID's Write ACR must be set to NEVER*

4.2.1 PIV CHUID Data Elements

59. The CHUID shall include an expiration date that specifies when the card expires
60. The CHUID shall include a position sensitivity level
61. The container and data elements of the CHUID are specified in the table below:

CHUID Container		Buffer EF: **3000**			Read ACR: **Always** Write ACR: **Never**
Data Element	**Tag**	**Type**	**Max Byte**	**Len**	**Description**
Buffer Length	EE	Fixed	2	2	Per GSC-IS Section 8.3
FASC-N	30	Fixed	25	25	*See PACS*
Agency Code	31	Fixed	4	4	Optional
Organization Identifier	32	Fixed	4	4	Optional
DUNS	33	Fixed	9	9	Optional
GUID	34	Fixed	16	16	Optional
Expiration Date	35	Fixed	8	8	YYYYMM??:
Position Sensitivity	36	Fixed	1	1	0x01 to 0x04
RFU	37-3C			TBD	Optional
Authentication Key Map	3D	Variable	TBD	TBD	Optional
Asymmetric signature	3E	Variable	TBD		*See below*
Error Detection Code	FE	LRC	1	1	Optional

4.2.2 Asymmetric Signature Field in CHUID

62. The asymmetric signature shall be formatted shall be formatted as a Cryptographic Syntax Message (CMS) external digital signature
63. The asymmetric signature shall be computed over the entire contents of the CHUID, excluding the CHUID asymmetric signature itself
64. The asymmetric signature shall be generated by the IA using the IA's PKI private key
65. Allowed algorithms and key sizes for the asymmetric signature are as follows:

	Algorithm	**First permitted issue date**	**Last permitted expiration date**
Public Key Algorithms & Key Sizes	RSA 1024	1/1/2005	12/31/2010
	RSA 2048	1/1/2005	?
	ECDSA 160	1/1/2005	12/31/2010
	ECDSA 224	1/1/2005	?
Hash Algorithms	SHA-1	1/1/2005	12/31/2007
	SHA-224	1/1/2005	12/31/2010
	SHA-256	1/1/2005	?

66. The asymmetric digital signature shall be constructed as follows:
    - Content shall be encoded *SignedData*
    - Certificates and CRLs shall not be included in message
    - *SignerInfo*s shall be present and include a single *SignerInfo*
    - The *SignerInfo* shall:
        1. Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
        2. Specify the Digest Algorithm
        3. Include the digital signature
67. The public key required to verify the asymmetric signature shall be carried on the PIV in a X.509 certificate:
68. The certificate shall be a digital signature certificate issued under [COMMON]
69. The certificate shall meet the format and infrastructure requirements of 4.3

4.3 Cryptographic Specifications

70. The PIV card must support at least one public/private key pair and certificate
71. The PIV card must perform all private key cryptographic operations on card
72. The PIV card must support key pair generation
73. The PIV card must support importation and storage of X.509 certificates
74. Public/private keys and algorithms shall be one of:

			Last permitted expiration date	
Algorithm	**Key Size**	**First permitted issue date**	**Everything but Digital Sign**	**Digital Signature**
RSA/DSA	1024	1/1/2005	12/31/2010	12/31/2008
RSA/DSA	2048	1/1/2005	?	?
ECDSA	160	1/1/2005	12/31/2010	12/31/2008
ECDSA	224	1/1/2005	?	?

75. No cryptographic operations are allowed through the contactless interface, with the singular of operations using the Local Authentication Key
76. The required and optional PIV keys are as follows:

Key Type	**PK or SK**	**Req or O**	**PIN or Bio Activation**	**Key Gen**	**Export**	**Interface(s)**
PIV Authentication	PK	Req	no	On Card	no	Contact Only
Local Authentication	Either	O	no	?	no	Either
Digital Signature	PK	O	YES	On Card	no	Contact Only
Key Management	PK	O	no	Either	?	Contact Only
Card Management	SK	O	?	Imported	?	Contact Only

77. Cross-Agency Interoperability is NOT a goal for Local Authentication Key

Since this is the only key that can be invoked over the contactless interface, this restricts all cryptographically secured cross agency interoperability to the contact interface.

78. All PIV cryptographic keys shall be generated within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above
79. All PIV cryptographic keys shall be stored within a FIPS 140-2 validated cryptomodule with overall validation at Level 2 or above and physical security validation at Level 3 or above
80. Algorithms and key sizes are as follows:

Algorithm	First permitted issue date	Last permitted expiration date	
		Everything but Digital Sign	Digital Signature
Two Key Triple-DES (TDEA2)	1/1/2005	12/31/2010	n/a
Three Key Triple DES (TDEA3)	1/1/2005	?	n/a
AES-128	1/1/2005	?	n/a
AES-192	1/1/2005	?	n/a
AES-256	1/1/2005	?	n/a
RSA/DSA 1024	1/1/2005	12/31/2010	12/31/2008
RSA/DSA 2048	1/1/2005	?	?
ECDSA 160	1/1/2005	12/31/2010	12/31/2008
ECDSA 224	1/1/2005	?	?
RSA/D-H 1024	1/1/2005	12/31/2008	n/a
RSA/D-H 2048	1/1/2005	?	n/a
ECDH 160	1/1/2005	12/31/2008	n/a
ECDH 224	1/1/2005	?	n/a

81. Certificate requirements are as follows:

		Authentication	Digital Signature	Key Management
Certificate Type		X.509	X.509	X.509
Expire on or before card?		Yes	?	?
Special Requirement		FASC-N in subject alternative name extension	-	-
Algorithm	**First permitted issue date**	**Last permitted expiration date**	**Last permitted expiration date**	**Last permitted expiration date**
RSA/DSA 1024	1/1/2005	12/31/2010	12/31/2007	12/31/2007
RSA/DSA 2048	1/1/2005	?	?	
ECDSA 160	1/1/2005	12/31/2010	12/31/2007	12/31/2007
ECDSA 224	1/1/2005	?	?	

4.4 Biometric Specifications

82. Biometric data shall be collected and used as follows:
    - Ten fingerprints, to support law enforcement check during the application process
    - Two electronic fingerprints, to be stored on the card for automatic verification
    - An electronic facial image, to be stored on the card for alternate identity verification

83. Fingerprints shall be the primary biometric used in the PIV system
84. Fingerprint preference, in decreasing order, is: index, thumb, middle, ring, and little fingers
85. The two fingerprints should not be from the same hand
86. 1-to-many fingerprint matching shall be performed during the application process
87. 1-to-1 fingerprint matching shall be performed during PIV identity verification
88. Biometric data on a PIV card may only be activated (1) from an activated card (2) through the contact interface

4.4.1 PIV Registration [Biometric Enrollment] and Issuance

89. PIV registration requires a 1-to-many biometric identification search to (1) detect duplicate credentialing and (2) perform background screening
90. Biometric data for 1-to-many identification search shall consist of ten "slap" fingerprints
91. Biometric data (2 fingerprints and 1 face) shall be embedded in the PIV card during personalization
92. All biometric data on the PIV card shall be digitally signed by the IA

4.4.2 Fingerprint Representation

93. Fingerprint images compliant with ANSI/NIST-ITL 1-2000 shall be used for PIV biometric enrollment
94. Fingerprint images compliant with ANSI/NIST-ITL 381-2004 shall be stored on the card for PIV identity verification

4.4.3 Fingerprint Requirements for Biometric Enrollment

Many technical requirements that do not impact policy. Omitted.

4.4.4 Fingerprint Requirements for Identity Verification

Technical requirements that do not impact policy. Omitted.

4.4.5 Facial Representation

95. Facial images are used for :
    - When fingerprints are unavailable
    - Multimodal applications that require face as well as fingerprint to lower FAR
    - Visual inspection

96. Facial images must comply with ANSI/INCITS 385-2004

4.4.5.1 Image Type

97. PIV implementations shall locate eyes, then rotate or translate image to conform to Token Geometry

4.4.5.2 Expression

98. PIV card facial image shall be acquired from applicant with neutral facial expression

4.4.5.3 Image Color Space

99. Image data shall be encoded in the YUV color space with 422 chromatic subsampling

4.4.5.4 Resolution

100. The PIV card image shall have an eye-to-eye resolution of at least 120 pixels
101. A [unspecified] higher resolution shall be used if the card has sufficient storage capacity
102. Images shall be acquired such that the native resolution is greater than or equal to 120 pixels
103. Acquisition at lower levels with interpolation shall not be applied
104. Scaling of images from larger sizes to achieve 120 pixels shall be done in one step

4.4.5.5 Compression

105. PIV images shall be compressed using the baseline JPEG compression algorithm using a 30:1 compression ratio
106. Images shall be acquired in raw form
107. Images shall not at any intermediate stage way be compressed in any way other than as mandated for final Token image
108. Image acquisition system should not apply compression before eye-location, scaling, rotation, and translation operations are performed during preparation of the Token image
109. Facial image properties shall be as follows:

Properties of the token 120 image	Value
Eye-to-eye resolution	120 pixels
Image width	480 pixels
Image height	640 pixels
Inner region width	384 pixels
Inner region height	480 pixels
Total image area	307,200 pixels
Uncompressed data sizeYUV422 color space	460,800 bytes
Baseline JPEG compression	30:1 ratio
Storage required after compression	15,360 bytes

The figures provided indicate that each pixel requires 1.5 bytes of storage. If each pixel actually requires only 1 byte, the storage required after compression is reduced to 10,240 bytes

4.4.5.6 Distortion

110. Image acquisition systems shall follow guidelines in Section A8 of ANSI/INCITS 385 to produce a standard radial distortion

4.4.5.7 Background

111. PIV card image shall be acquired with subject in front of a uniform background

4.4.5.8 Quality

112. During enrollment, an automate assessment of [acquired] facial image quality shall be made while the applicant is present
113. A quality measuring implementation shall produce a value in the range of 1 to 100 as follows:

Value	Meaning	Action
81-100	No defects are present	Accept and enroll
61-90	Minor defects are present	Accept and enroll
41-60	Some tolerable defects are present	Reacquire unless timeout has been reached. If timeout reached, acquire best image
21-40	Unacceptable for enrollment when reacquisition is possible	Reacquire unless timeout has been reached. If presentation limit has been reached, inspect equipment and environment. Require subject to return.
1-20	Unacceptable for enrollment and one-to-many operations	Reacquire. If presentation limit has been reached, inspect equipment and environment, then seek vendor support if no apparent cause of failure. Require subject to return later.

Not defined: timeout *and* presentation limit

114. Quality values developed and assigned such that they are ultimately indicative of true and/or false accept rates in verification or identification.
115. Low quality values shall be reported if:
    - Face is non-frontal or rotated
    - Face is not located centrally
    - Face is cropped
    - Image is blurred
    - Image is over or under exposed
    - Image is compressed in any inferior manner to that specified in this standard

4.4.5.9 Protection of Biometrics

116. PIV card must protect biometric data during storage
117. All biometric data shall be signed with CMS external signature
118. The digital signature shall be computed over a concatenation of the following elements:
    - CBEFF header Version (if present)
    - Patron Header Version
    - Biometric Type (if present)
    - Record Data Type (if present)
    - Record Purpose (if present)
    - Record Data Quality (if present)
    - Creation Date (if present)
    - Creator (if present)
    - Biometric Specific Memory Block (BSMB) Format Owner
    - BSMB Format Type
    - BSMB
119. The CMS external digital signature shall be constructed as follows:
    - Content shall be *SignedData*
    - Certificates and CRLs shall not be included in message
    - *SignerInfo*s shall be present and include a single *SignerInfo*
    - The *SignerInfo* shall:
        1. Use the *issuerAndSerialNumber* choice for *SignerIdentifier*
        2. The authentication attributes shall be present and include a *serialnumber* attribute with the FASC-N for the PIV card
        3. Include the digital signature
    - Additional information such as the cardholder's name or distinguished name in the cardholder's PKI certificates may be included in the *SignerInfo* authenticated attributes

4.5 Card Reader Specifications

4.5.1 Contact Reader Specifications

120. Contact readers shall conform to ISO/IEC 7816 for card-to-reader interface
121. Contact readers shall conform to PC/SC for reader-to-host system interface

This may be an issue for contact readers attached to a PACS control panel rather than a general purpose desktop computing system

4.5.2 Contactless Reader Specifications

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

4.5.3 PIN Pad Specifications

124. PIV cards may be activated through the contact interface by the card holder using the PIN

This phrasing suggests that the PIV card may NOT be activated through the contactless interface, though that is not specified in 4.1.5

125. Where used for physical access, the PIN pad shall be incorporated into the reader
126. Where used for physical access, the PIN pad may be incorporated into the reader or the PIN may be entered using the computer keyboard

Graduated Criteria

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

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

Graduated criteria should are provided as follows:

a. Claimed Identity Verification

Level	Criteria	Description
ID1	I-9 Doc Check	Check two I-9 documents, at least one of which is a picture ID
ID2	Name Check	Check against available public and private record repositories,
ID3	SSN Check	Check against available public and private record repositories,
ID4	LEO Check	Law enforcement fingerprint check. Verifying that, if the applicant's fingerprints appear in records within the criminal justice system, that the identity corresponding to those records matches the identity given on the PIV application
ID5	Primary Reference Check	Primary references (those provided by applicant) confirm applicant's identity based on photo taken during registration. (Identity only, not trustworthiness)
ID6	Secondary Reference Check	Secondary references (not provided by applicant) confirm applicant's identity based on photo taken during registration. (Identity only, not trustworthiness)

b.1 Resistance to Tampering & Counterfeiting: Graphical		
Level	Criteria	Description
G1	Similar Appearance	Departments & agencies are free to follow general guidelines, so that all PIVs have about the same graphical elements in about the same place using about the same fonts and sizes (E.g FIPS 201 PUBLIC Draft section 4.1.4)
G2	Uniform Appearance	PIVs adhere to a tight standard for graphical appearance, including a clear specification of: • Background color & pattern • Zone location to within a tight tolerance (.01 inch) • Font sizes (eliminate "minimum" where possible) • Additional printing (what is allowed & where)
G3	+ Security Feature	Uniform Appearance + All PIVs have a uniform and recognizable security feature (e.g. OVD/OVI)
G4	+ Multiple Security Features	Uniform Appearance + All PIVs have a uniform set of recognizable and testable security features. Possibilities include: • OVD/OVI • Guilloche • Very fine line • Micro printing • Laser engraving • Laser printing • UV inks • Hidden word Final set of required security features is TBD. This list is closely held and shared with qualified manufacturers on a "need to know" basis.

Resistance to fraud, tampering, counterfeiting, and exploitation:

- Electrical criteria should address cryptographic, biometric, demographic and cardholder knowledge mechanisms features at each graduated level
- Electrical criteria should also address what data elements can be rewritten after card issuance and the controls and security mechanisms that are applied

Rapid electronic authentication:

c.1 Rapid Electronic Authentication: PIV Auth		
Level	Criteria	Description
PA1	Data Present	Issuer-signed data is found on the PIV
PA2	+ PIV Challenge	Above + PIV demonstrates it knows the authentication secret (e.g. it signs a random challenge with the PIV Authentication private key, which the reader then verifies with the public key)
PA3	+ Cert Check	Above + Reader verifies authenticity of PIV Auth Cert (by verifying the issuers digital signature)
PA4	+ Expired Check	Above + Reader checks the expiration date in the certificate
PA5	+ CRL Check	Above + Reader checks most recent CRL from issuer to verify certificate has not been revoked
PA6	+ issuer Check	Above + Reader checks real time with issuer service to verify that certificate is still valid

c.2 Rapid Electronic Authentication: Cardholder Auth		
Level	Criteria	Description
CA1	Possession	Cardholder is in possession of the card
CA2	Card + PIN	The cardholder has successfully entered the PIN
CA3	Card + Bio	The cardholder has successfully passed a biometric match
CA4	Card + Pin + Bio	The card holder has successfully entered the PIN and passed a biometric match.
Note: This scheme applies whether the authentication is performed by the card or by an external entity (reader, PC, door controller…) *The guiding principal is that the authenticating entity must perform the match.* Thus: • Card-based: The card must perform the PIN validation and/or biometric match. • External Auth: External entity must perform the PIN validation and/or biometric match.		

d. Issuer Accreditation		
Level	Criteria	Description

Accreditation of issuers – should include requirements for:

- Personnel security for Approving Official (AO), Registration Authority (RA), and Issuing Authority (IA)
- Physical security for areas containing personalization equipment and storing cardstock
- Audit requirements for cardstock prior to personalization
- Audit requirements for personalized PIV cards through issuance
- Procedures for securing issuance equipment and cardstock at the close of business.