

FICAM PACS

Master Test Procedures

VERSION 0.1.0



DRAFT

FIPS 201 EVALUATION PROGRAM

January 23, 2013

Office of Government wide Policy Office of Technology Strategy Identity Management Division Washington, DC 20405

Document History

Status	Version	Date	Comment	Audience
Draft	0.0.1	12/08/12	Document creation	Limited
Draft	0.0.2	1/8/13	First team edit	Limited
Draft	0.0.3	1/8/13	Second team edit	Limited
Draft	0.0.4	1/13/13	Initial basic QA	Limited
Draft	0.0.5	1/20/13	Revisions per QA	Limited
Draft	0.0.6	1/22/13	Added cryptography testing	Limited
Draft	0.1.0	1/23/13	Team review	EPTWG



Table of Contents

1	In	troduct	tion	1
	1.1	Test	Scoring Guidelines	1
	1.2	Syst	em Under Test	1
	1.3	Test	Components	2
	1.4	PKI I	Used in Test	3
2	Αι	uthenti	cation at Time of Registration Test Cases	5
	2.1	Sign	ature Verification	5
	2.:	1.1	Valid Signature PIV	5
	2.:	1.2	Valid Signature PIV-I	5
	2.:	1.3	Invalid CA Signature	5
	2.:	1.4	Invalid End Entity	5
	2.2	Cert	ificate Validity Periods	6
	2.:	2.1	Invalid CA notBefore Date	6
	2.:	2.2	Invalid End Entity certificate notBefore Date	6
	2.:	2.3	Invalid CA notAfter Date	6
	2.:	2.4	Invalid End Entity certificate notAfter Date	6
	2.3	Nan	ne Chaining	6
	2.3	3.1	Invalid Name Chaining End Entity Certificate	6
	2.4	Basi	c Constraints Verification	7
	2.	4.1	Invalid Missing Basic Constraints	7
	2.4	4.2	Invalid CA False Critical	7
	2.4	4.3	Invalid CA False not Critical	7
	2.4	4.4	Invalid pathLenConstraint	7
	2.5	Key	Usage Verification	8
	2.	5.1	Invalid keyUsage Critical keyCertSign False	8
	2.	5.2	Valid keyUsage Not Critical	8
	2.	5.3	Invalid keyUsage Critical cRLSign False	8
	2.6	Cert	ificate Policies	8
	2.0	6.1	Explicit Certificate Policy Required and Present	8
	2.0	6.2	Explicit Certificate Policy Required and not Present	9
	2.0	6.3	Explicit Certificate Policy Required Across Bridge and Present in End Entity Certificate	9

2.6.	.4	Explicit Certificate Policy Required Across Bridge and not Present in End Entity Certifica 10	te
2.6. End	_	Explicit Certificate Policy Required Across Bridge and Present in Path, but not Present in Yertificate	
2.7	Inhil	bit Policy Mappings	11
2.7.	.1	Invalid inhibitPolicyMapping	11
2.8	Nan	ne Constraints	11
2.8.	.1	Valid DN nameConstraints	. 11
2.8.	.2	Invalid DN nameConstraints	11
2.8.	.3	Invalid DN nameConstraints invalid SAN	12
2.9	Cert	ificate Revocation Tests (CRL)	13
2.9.	.1	Unavailable CRL	13
2.9.	.2	Revoked CA	13
2.9.	.3	Revoked End Entity	13
2.9.	.4	Invalid CRL Signature	13
2.9.	.5	Invalid CRL Issuer Name	13
2.9.	.6	Old CRL nextUpdate	13
2.9.	.7	Invalid notBefore Date	13
2.9.	.8	Invalid Distribution Point	13
2.10	CHU	IID Verification	14
2.10	0.1	Invalid CHUID signature	14
2.10	0.2	Expired CHUID signer	14
2.10	0.3	Expired CHUID	14
2.10	0.4	FASC-N != in CHUID	14
2.10	0.5	UUID != in CHUID	14
2.11	Faci	al Image Verification	14
2.1	1.1	Invalid Facial Image signature	14
2.12	FINC	GERPRINT Verification	15
2.12	2.1	Invalid Fingerprint signature	15
2.12	2.2	Valid Bio	15
2.12	2.3	Invalid Bio	15
2.13	Secu	urity Object Verification	15

2.	13.1	Invalid Security Object signature	15
2.14	ocs	SP Response Checking	16
2.	14.1	Good OCSP Signer	16
2.	14.2	Expired OCSP Signer	16
2.	14.3	Revoked OCSP Signer with PKIX_OCSP_NOCHECK present	16
2.	14.4	Revoked OCSP Signer with PKIX_OCSP_NOCHECK not present	16
2.	14.5	Invalid OCSP Signer	16
2.15	Inte	properability Testing	16
2.16	Cry	otographic Testing	16
2.	16.1	RSA PKCS#1 v1.5 (1024)	16
2.	16.2	RSA PKCS#1 v1.5 (2048)	16
2.	16.3	RSA PKCS#1 v1.5 (3072)	17
2.	16.4	RSASSA-PSS (1024)	17
2.	16.5	RSASSA-PSS (2048)	17
2.	16.6	RSASSA-PSS (3072)	17
2.	16.7	RSA key transport (1024)	17
2.	16.8	RSA key transport (2048)	17
2.	16.9	RSA key transport (3072)	17
2.	16.10	ECDSA (P-256)	17
2.	16.11	ECDSA (P-384)	17
2.	16.12	ECDH (P-256)	17
2.	16.13	ECDH (P-384)	17
2.	16.14	SHA-1	17
2.	16.15	SHA-256	17
2.	16.16	SHA-384	17
2.	16.17	2TDEA	17
2.	16.18	3TDEA	18
2.	16.19	AES-128	18
2.	16.20	AES-192	18
2.	16.21	AES-256	18
2.	16.22	RSA key exponent 65,537 (2^16+1)	18
2.	16.23	RSA key exponent (2^256-1)	18

3	Auther	ntication at Time of Access Test Cases	19
	3.1 Si	gnature Verification	19
	3.1.1	Valid Signature PIV	19
	3.1.2	Valid Signatures PIV-I	19
	3.1.3	Invalid CA Signature	19
	3.1.4	Invalid End Entity	19
	3.2 C	ertificate Validity Periods	20
	3.2.1	Invalid CA notBefore Date	20
	3.2.2	Invalid End Entity certificate notBefore Date	20
	3.2.3	Invalid CA notAfter Date	20
	3.2.4	Invalid End Entity certificate notAfter Date	20
	3.3 N	ame Chaining	20
	3.3.1	Invalid Name Chaining End Entity Certificate	20
	3.4 Ba	asic Constraints Verification	21
	3.4.1	Invalid Missing Basic Constraints	21
	3.4.2	Invalid CA False Critical	21
	3.4.3	Invalid CA False not Critical	21
	3.4.4	Invalid pathLenConstraint	21
	3.5 K	ey Usage Verification	22
	3.5.1	Invalid keyUsage Critical keyCertSign False	22
	3.5.2	Valid keyUsage Not Critical	22
	3.5.3	Invalid keyUsage Critical cRLSign False	22
	3.6 C	ertificate Policies	23
	3.6.1	Explicit Certificate Policy Required and Present	23
	3.6.2	Explicit Certificate Policy Required and not Present	23
	3.6.3	Explicit Certificate Policy Required Across Bridge and Present in End Entity Certificate	ate 23
	3.6.4	Explicit Certificate Policy Required Across Bridge and not Present in End Entity Cert 24	tificate
	3.6.5 End En	Explicit Certificate Policy Required Across Bridge and Present in Path, but not Presentity Certificate	
	3.7 In	hibit Policy Mappings	25
	3.7.1	Invalid inhibitPolicyMapping	25

3	.8 8.	lame Constraints	25
	3.8.1	Valid DN nameConstraints	25
	3.8.2	Invalid DN nameConstraints	25
	3.8.3	Invalid DN nameConstraints invalid SAN	26
3	.9 (Certificate Revocation Tests (CRL)	26
	3.9.1	Unavailable CRL	26
	3.9.2	Revoked CA	26
	3.9.3	Revoked End Entity	26
	3.9.4	Invalid CRL Signature	26
	3.9.5	Invalid CRL Issuer Name	26
	3.9.6	Old CRL nextUpdate	26
	3.9.7	Invalid notBefore Date	27
	3.9.8	Invalid Distribution Point	27
3	.10 (CHUID Verification	27
	3.10.1	Invalid CHUID signature	27
	3.10.2	2 Expired CHUID signer	27
	3.10.3	B Expired CHUID	27
	3.10.4	FASC-N != in CHUID	27
	3.10.5	5 UUID != in CHUID	27
3	.11 F	acial Image Verification	28
	3.11.1	Invalid Facial Image signature	28
3	.12 F	INGERPRINT Verification	28
	3.12.1	Invalid Fingerprint signature	28
	3.12.2	2 Valid Bio	28
	3.12.3	B Invalid Bio	28
3	.13 S	ecurity Object Verification	28
	3.13.1	Invalid Security Object signature	28
3	.14 (DCSP Response Checking	29
	3.14.1	Good OCSP Signer	29
	3.14.2	Expired OCSP Signer	29
	3.14.3	Revoked OCSP Signer with PKIX_OCSP_NOCHECK present	29
	3.14.4	Revoked OCSP Signer with PKIX_OCSP_NOCHECK not present	29

FICAM PACS Master Te	est Procedures
----------------------	----------------

v0.1.0

	3.14.5	Invalid OCSP Signer	29
	3.15 Inte	roperability Testing	29
	3.16 Cryp	otographic Testing	29
	3.16.1	RSA PKCS#1 v1.5 (1024)	29
	3.16.2	RSA PKCS#1 v1.5 (2048)	29
	3.16.3	RSA PKCS#1 v1.5 (3072)	30
	3.16.4	RSASSA-PSS (1024)	30
	3.16.5	RSASSA-PSS (2048)	30
	3.16.6	RSASSA-PSS (3072)	30
	3.16.7	RSA key transport (1024)	30
	3.16.8	RSA key transport (2048)	30
	3.16.9	RSA key transport (3072)	30
	3.16.10	ECDSA (P-256)	30
	3.16.11	ECDSA (P-384)	30
	3.16.12	ECDH (P-256)	30
	3.16.13	ECDH (P-384)	30
	3.16.14	SHA-1	30
	3.16.15	SHA-256	30
	3.16.16	SHA-384	30
	3.16.17	2TDEA	30
	3.16.18	3TDEA	30
	3.16.19	AES-128	31
	3.16.20	AES-192	31
	3.16.21	AES-256	31
	3.16.22	RSA key exponent 65,537 (2^16+1)	31
	3.16.23	RSA key exponent (2^256-1)	31
	3.17 Con	tinuity of Operations Testing	32
	3.17.1	Network Connectivity Loss to Panel	32
	3.17.2	Network Connectivity Loss to Server	32
	3.17.3	Services Stopped on Server	32
	3.17.4	Power Loss to Panel	33
4	PACS Des	sign Use Cases	34

4.1	Secu	rity Boundaries	34
4.	1.1	Attack side processing 1	34
4.	1.2	Attack side processing 2	34
4.	1.3	Attack side processing 3	34
4.2	Regi	stering Physical Access Privileges	35
4.	2.1	Populations 1	35
4.	2.2	Populations 2	35
4.	2.3	Populations 3	35
4.	2.4	Populations 4	35
4.	2.5	Valid Registration	35
4.	2.6	Valid Registration 2	35
4.	2.7	Valid Registration 3	36
4.	2.8	Binding to Bearer 1	36
4.	2.9	Binding to Bearer 2	36
4.	2.10	Policy Constraints	36
4.	2.11	Workflow	36
4.3	Valid	lation at Time of Access	37
4.	3.1	Signed CHUID	37
4.	3.2	Card Authentication Key	37
4.	3.3	PIV Authentication Key + PIN	37
4.	3.4	PIV Authentication Key + PIN + BIO	37
4.	3.5	PIN to PACS	37
4.4	Port	al Hardware	38
4.	4.1	Readers 1	38
4.	4.2	Readers 2	38
4.	4.3	Readers 3	38
4.	4.4	Readers 4	38
4.	4.5	Readers 5	39
4.	4.6	Readers 6	39
4.5	Audi	ting and Logging	39
4.	5.1	Auditing 1	39
4.	5.2	Auditing 2	39

FICAM PACS N	Master Test Procedures	v0.1.0
4.5.3	Auditing 3	
4.5.4	Auditing 4	40
4.5.5	Auditing 5	40
4.5.6	Auditing 6	40
4.5.7	Auditing 7	40
4.5.8	Auditing 8	40
4.5.9	Auditing 9	40
4.5.10	Auditing 10	40
4.5.11	Auditing 11	40
4.5.12	Auditing 12	40
4.5.13	Auditing 13	
4.6 Seci	urity Certification and Accreditation	41
4.6.1	UL Assessment	41
4.6.2	FIPS 201-1	41
4.6.3	FIPS 140-2	41
4.7 Bior	metric in PACS	41
4.7.1	Biometric Encryption	
	erational Controls	
4.8.1	System Configuration	
4.8.2	Component Addressing	
4.8.3	Configuration Downloads	
4.0.5	Configuration Downloads	41
	List of Tables	
Table 1 - ICA	AM Test Cards Used in Test	2
Table 2 - PK	I Used in Test	3

1 1 Introduction

2 1.1 Test Scoring Guidelines

- 3 The following scoring guidelines are used by the Federal Identity, Credential, and Access Management
- 4 (FICAM) Test Lab for the FICAM Testing Program. There are two main families of test cases:
- **Security** A control directly impacting security of the system.
- Usability A control impacting end user system usability. Does not directly impact security.
- 7 For each test case evaluating a control (both Usability and Security), there are three possible
- 8 classifications:
- Mandatory All mandatory controls must be present and must work correctly. They are reported as Red (fail critical) / Green (pass).
- Optional Always tested. They are reported as Yellow (fail not critical) / Green (pass).
- Optional * These controls are part of the feature set of a given Product. They may be present. If present, it must work correctly and will be reported as Red (fail critical) / Green (pass). If not present, they will be reported as Yellow (fail not present).
- 15 The above scoring is done for each control test case for the FICAM Testing Program.
- 16 1.2 System Under Test
- 17 A full system tested by the FICAM Testing Program for a Physical Access Control System (PACS) includes
- the following components:

Component	Component Code	Make	Model	Software/Firmware Version
Head-End Server	Н			
PACS Panel	Н			
Validation System	V			
Secure Controller	V			
Door Reader	R			

1.3 Test Components

22 The following cards are used in the FICAM Testing Program.

- 1. Live PIV and PIV-I cards from various issuers.
- 2. ICAM Test Cards (detailed in *Table 1*)
- 3. ICAM PKI infrastructure (detailed in *Table 2*).
- 4. NIST PIV Test Cards.
- 5. DoD JITC CAC Test Cards.
 - 6. Full system under test, encompassing:
 - Reader for Access;
 - b. Validation System; and
 - c. PACS Head-End.

31 32

21

23

24

25

28

29

30

Table 1 - ICAM Test Cards Used in Test

ICAM Test Cards	Description	Threat Type
1	Golden PIV	None
2	Golden PIV-I	None
3	Placeholder for ECC card	TBD
4	Tampered CHUID	Manipulated Data
5	Tampered PIV and Card Authentication Certificates	Manipulated Data
6	Tampered PHOTO	Manipulated Data
7	Tampered FINGERPRINT	Manipulated Data
8	Tampered SECURITY OBJECT	Manipulated Data
9	Expired CHUID signer	Invalid Date
10	Expired certificate signer	Invalid Date
11	PIV Authentication Certificate expiring after CHUID	Invalid Date
12	Authentication certificates valid in future	Invalid Date
13	Expired authentication certificates	Invalid Date
14	Expired CHUID	Invalid Date
15	Valid CHUID copied from one card to another (PIV)	Copied Credential
16	Valid Card Authentication Certificate copied from one card to another (PIV)	Copied Credential
17	Valid PHOTO copied from one card to another (PIV)	Copied Credential
18	Valid FINGERPRINT copied from one card to another (PIV)	Copied Credential
19	Valid CHUID copied from one card to another (PIV-I)	Copied Credential
20	Valid Card Authentication Certificate copied from one card to another (PIV-I)	Copied Credential
21	Valid PHOTO copied from one card to another (PIV-I)	Copied Credential
22	Valid FINGERPRINT copied from one card to another (PIV-I)	Copied Credential
23	Private and Public Key mismatch	No Trusted Path
24	Revoked authentication certificates	Revoked
		Credential

35 1.4 PKI Used in Test

36

The following PKI infrastructure is used for the FICAM Testing Program:

37 Table 2 - PKI Used in Test

Path	Fault description	Operational group
Number		
1	Invalid CA Signature	Manipulated Data
2	Invalid CA notBefore Date	Revoked/Date Invalid
3	Invalid CA notAfter Date	Revoked/Date Invalid
4	Invalid Name Chaining	Standards Conformant Processing
5	Missing Basic Constraints	Standards Conformant Processing
6	Invalid CA False Critical	Manipulated Data
7	Invalid CA False not Critical	Standards Conformant Processing
8	Invalid pathLenConstraint	Standards Conformant Processing
9	keyUsage keyCertSign not set	Standards Conformant Processing
10	keyUsage Not Critical	Standards Conformant Processing
11	keyUsage Critical cRLSign False	Standards Conformant Processing
12	Invalid inhibitPolicyMapping	Standards Conformant Processing
13	Invalid DN nameConstraints	Standards Conformant Processing
14	Invalid Subject Alternatve Name	Standards Conformant Processing
15	Invalid Missing CRL	Standards Conformant Processing
16	Invalid Revoked CA	Revoked/Date Invalid
17	Invalid CRL Signature	Manipulated Data
18	Invalid CRL Issuer Name	Standards Conformant Processing
19	Invalid Old CRL nextUpdate	Revoked/Date Invalid
20	Invalid CRL notBefore Date	Revoked/Date Invalid
21	Invalid distributionPoint	Standards Conformant Processing
22	Valid requiredExplicitPolicy	Standards Conformant Processing
23	Invalid requiredExplicitPolicy	Standards Conformant Processing
24	Valid GeneralizedTime	PKI/Crypto Compatibility
25	Invalid GeneralizedTime	Standards Conformant Processing
26	ECC prime256v1	PKI/Crypto Compatibility
27	ECC secp384r1	PKI/Crypto Compatibility

Path Number	Fault description	Operational group
28	Invalid ECC Signature p256	Manipulated Data
29	Invalid Policy Mapping p256	Standards Conformant Processing
30	Invalid ECC Signature	Manipulated Data
31	Invalid Policy Mapping	Standards Conformant Processing
32	Invalid SKID	Standards Conformant Processing
33	Invalid AKID	Standards Conformant Processing
34	Invalid CRL format	Standards Conformant Processing
35	4096 RSA key	PKI/Crypto Compatibility

2 Authentication at Time of Registration Test Cases

40 2.1 Signature Verification

- 41 Applications must be able to verify digital signatures on each certificate in the certification path using
- 42 the public key from the previous certificate in the path. These test cases validate signatures in the
- 43 certificates found in the certification path.

Test		Components	Description	Test condition	Туре
2.1.1	Valid Signature PIV	н, V	Verify Product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	Card 1: PIV Golden Registers successfully.	Security – Mandatory
2.1.2	Valid Signature PIV-I	н, V	Verify Product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	Card 2: PIV-I Golden Registers successfully.	Security – Mandatory
2.1.3	Invalid CA Signature	V	Verify Product's ability to recognize invalid signature on an intermediate CA in the certification path.	Card 1: (Golden PIV Card) with Path 1 fails to register successfully.	Security – Mandatory
2.1.4	Invalid End Entity	V	Verify Product's ability to recognize invalid signature on the End Entity certificate.	Card 5: invalid PIV/Card Auth Signer fails to register successfully.	Security – Mandatory

45 2.2 Certificate Validity Periods

- 46 The Product must verify notBefore time of each certificate to be earlier than or equal to the current
- 47 time. The Product must also verify notAfter to time be to be later or equal to the current time. The
- 48 following tests validate notBefore and notAfter values in each certificate in the path.

Test		Components	Description	Test condition	Туре
n	nvalid CA notBefore Date	V	Verify Product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future.	Card 1: (Golden PIV Card) with Path 2 fails to register successfully.	Security – Mandatory
E C n	nvalid End Entity certificate notBefore Date	٧	Verify Product's ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future.	Card 12: (Certs not yet valid) fails to register successfully.	Security – Mandatory
n	nvalid CA notAfter Date	V	Verify Product's ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past.	Card 1: (Golden PIV Card) with Path 3 fails to register successfully.	Security – Mandatory
E c n	nvalid End Entity certificate notAfter Date	v	Verify Product's ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past.	Card 13: (Certs Expired) fails to register successfully.	Security – Mandatory

2.3 Name Chaining

- 50 The purpose of the following test is to verify the Product's ability to check that names chain correctly
- 51 within certification path.

Test	Components	Description	Test condition	Туре
2.3.1 Invalid Name Chaining End Entity Certificate	V	Verify Product's ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	Card 1: (Golden PIV Card) with Path 4 fails to register successfully.	Security – Mandatory

56 57

2.4 Basic Constraints Verification

Test in this sections are used to verify that the Product correctly processes **basicConstraints** extension.

Test	Components	Description	Test condition	Туре
2.4.1 Invalid Missing Basic Constraints	V	Verify Product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Card 1: (Golden PIV Card) with Path 5 fails to register successfully.	Security – Mandatory
2.4.2 Invalid CA False Critical	V	Verify Product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false.	Card 1: (Golden PIV Card) with Path 6 fails to register successfully.	Security - Optional
2.4.3 Invalid CA False not Critical	V	Verify Product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false.	Card 1: (Golden PIV Card) with Path 7 fails to register successfully.	Security - Optional
2.4.4 Invalid pathLenConst raint	v	Verify Product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) with Path 8 fails to register successfully.	Security – Mandatory

58 2.5 Key Usage Verification

59

- Tests in this section verify the Product's ability to correctly process keyUsage extension in a certificate
- 60 when subject public key is to be used to verify signatures on certificates and CRLs.

Test		Components	Description	Test condition	Туре
2.5.1	Invalid keyUsage Critical keyCertSign False	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false.	Card 1: (Golden PIV Card) with Path 9 fails to register successfully.	Security – Mandatory
2.5.2	Valid keyUsage Not Critical	V	Verify Product's ability to recognize when the intermediate certificate includes a non-critical keyUsage extension.	Card 1: (Golden PIV Card) with Path 10 fails to register successfully.	Security – Mandatory
2.5.3	Invalid keyUsage Critical cRLSign False	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which cRLSign is false.	Card 1: (Golden PIV Card) with Path 11 fails to register successfully.	Security – Mandatory

61 2.6 Certificate Policies

62 Tests in this section verify the Product's ability to correctly process **certificatePolicies** extension.

Test		Components	Description	Test condition	Туре
2.6.1	Explicit Certificate Policy Required and Present	v	With the trust anchor set to Commercial Root check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate path. The explicit policy will be set to PIV-I Hardware.	Production PIV-I registers successfully.	Security – Mandatory

Test	Components	Description	Test condition	Туре
2.6.2 Explicit Certificate Policy Required and not Present	i V	With the trust anchor set to Commercial Root check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate path. The explicit policy will be set to an arbitrary value that is not present in the certificate path (e.g., OID value 1.2.3.4).	Production PIV-I fails to register.	Security – Mandatory
2.6.3 Explicit Certificate Policy Required Across Bridg and Present in End Entity Certificate		With the trust anchor set so the certificate path requires trust across the Commercial Bridge to Federal Common Policy CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and present in the certificate in a bridged trust environment. The explicit policy will be set to PIV-I Hardware. Test Condition: production PIV-I passes.	Production PIV-I registers successfully.	Security – Mandatory

Test	Components	Description	Test condition	Туре
2.6.4 Explicit Certificate Policy Required Across Bridge and not Present in End Entity Certificate	V	With the trust anchor set so the certificate path requires trust across the Commercial Bridge Federal Common Policy CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4).	Production PIV-I fails to register.	Security – Mandatory
2.6.5 Explicit Certificate Policy Required Across Bridge and Present in Path, but not Present in End Entity Certificate	V	With Federal Common Policy CA anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate — however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (e.g., High Hardware).	Production PIV-I fails to register.	Security – Mandatory

2.7 Inhibit Policy Mappings

- The test in this section verifies the application's ability to process the inihibitPolicyMapping field of the
- 67 **policyConstraints** extension and to verify that policy mappings are processed correctly after policy
- 68 mapping has been inhibited.

65 66

69

Test	Interface	Description	Test condition	Туре
2.7.1 Invalid inhibitPolicyM apping	V	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B.	Card 1: (Golden PIV Card) with Path 12 fails to register successfully.	Security – Mandatory

2.8 Name Constraints

70 Tests in this section verify the Product's ability to correctly process **nameConstraints** extension.

Test	Components	Description	Test condition	Туре
2.8.1 Valid DN nameConstrai	v	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) access grant succeeds.	Security – Mandatory
2.8.2 Invalid DN nameConstrai nts	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) with Path 13 fails to register successfully.	Security – Mandatory

Test	Components	Description	Test condition	Туре
2.8.3 Invalid DN nameConstrai nts invalid SAN	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	Card 1: (Golden PIV Card) with Path 14 fails to register successfully.	Security – Mandatory

2.9 Certificate Revocation Tests (CRL)

Tests in this section verify the Product's ability to retrieve and process valid revocation data for each

75 certificate in the path via CRL.

73

Test	Comp	onents	Description	Test condition	Туре
2.9.1 Unavaila CRL		/	The system recognizes when no revocation information is available for the End Entity certificate.	Card 1: (Golden PIV Card) with Path 15 fails to register successfully.	Security – Mandatory
2.9.2 Revoked		/	The system recognizes when a second intermediate CA certificate is revoked.	Card 1: (Golden PIV Card) with Path 16 fails to register successfully.	Security – Mandatory
2.9.3 Revoked Entity		/	The system recognizes when the End Entity certificate is revoked.	Card 24: (Revoked status) fails to register successfully.	Security – Mandatory
2.9.4 Invalid (Signatur	Δ	/	The System Recognizes when a CRL Signature is Invalid.	Card 1: (Golden PIV Card) with Path 17 fails to register successfully.	Security – Mandatory
2.9.5 Invalid (Issuer Na	ame	,	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.	Card 1: (Golden PIV Card) with Path 18 fails to register successfully.	Security – Mandatory
2.9.6 Old CRL nextUpd		/	The system recognizes when a certificate in the path points to a CRL with an expired nextUpdate value.	Card 1: (Golden PIV Card) with Path 19 fails to register successfully.	Security – Mandatory
2.9.7 Invalid notBefor Date	-	,	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	Card 1: (Golden PIV Card) with Path 20 fails to register successfully.	Security – Mandatory
2.9.8 Invalid Distribut Point	ion	/	The system recognizes when a certificate in the path has an incorrect distribution point.	Card 1: (Golden PIV Card) with Path 21 fails to register successfully.	Security – Mandatory

78 2.10 CHUID Verification

79 Tests in this section verify the system's ability to correctly verify CHUID's validity.

Test	Components	Description	Test condition	Туре
2.10.1Invalid CHUID signature	V	The system recognizes when the CHUID signature is invalid and does not verify.	Card 4: (Invalid CHUID Signature) fails to register successfully.	Security – Mandatory
2.10.2Expired CHUID signer	V	The system recognizes when the CHUID signer certificate is expired.	Card 9: (Expired CHUID signer) fails to register successfully.	Security – Mandatory
2.10.3Expired CHUID	V	The system recognizes when the CHUID is expired.	Card 14: (Card Expired) fails to register successfully.	Security – Mandatory
2.10.4FASC-N != in CHUID	V	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.	Card 15: (FASC-N in CHUID !=) fails to register successfully.	Security – Mandatory
2.10.5UUID != in CHUID	V	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV Auth Cert.	Card 19: (UUID in CHUID !=) fails to register successfully.	Security – Mandatory

80 2.11 Facial Image Verification

- 81 The test in this section verifies the Product's ability to correctly verify Facial Image object. Test cards
- 82 use CHUID Signer Certificate for biometric objects.

Test	Components	Description	Test condition	Туре
2.11.1Invalid Facial Image signature	v	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) fails to register successfully.	Security – Mandatory

84 2.12 FINGERPRINT Verification

Tests in this section verify the Product's ability to correctly verify FINGERPRINT object. Test cards use CHUID Signer Certificate for biometric objects.

Test	Components	Description	Test condition	Туре
2.12.1 Invalid Fingerprint signature	V	The system recognizes when the Fingerprint signature is invalid and does not verify.	Card 7: (bad fingerprint signature) fails to register successfully.	Security – Mandatory
2.12.2 Valid Bio	Н, V	With fingerprint checking enabled, a good credential is presented to the system with a valid fingerprint.	PIV-I registers successfully.	Security – Mandatory
2.12.3 Invalid Bio	н, v	With fingerprint checking enabled, a good credential is presented to the system with an invalid fingerprint.	PIV-I fails to register.	Security – Mandatory

2.13 Security Object Verification

88 The test in this section verifies the Product's ability to correctly verify Security Object.

Test	Components	Description	Test condition	Туре
2.13.1 Invalid Security Object signature	v	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) fails to register successfully.	Security – Mandatory

87

85

2.14 OCSP Response Checking

90

91 Tests in this section verify the Product's ability to validate OCSP responses.

Test	Components	Description	Test condition	Туре
2.14.1Good OCSP Signer	V	The system successfully validates a good credential using an OCSP response with a good signature.	Card 1: Golden PIV registers successfully.	Security – Mandatory
2.14.2Expired OCSP Signer	V	Validation fails using an OCSP response with an expired signature for a good card.	Card 1: Golden PIV fails to register successfully.	Security – Mandatory
2.14.3 Revoked OCSP Signer with PKIX_OCSP_ NOCHECK present	V	Validation succeeds using an OCSP response with a revoked signature for a good card with. PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV registers successfully.	Security – Mandatory
2.14.4Revoked OCSP Signer with PKIX_OCSP_ NOCHECK not present	V	Validation fails using an OCSP response with a revoked signature for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV fails to register successfully.	Security – Mandatory
2.14.5 Invalid OCSP Signer	V	Validation fails using an OCSP response with an malformed signature for a good card.	Card 1: Golden PIV fails to register successfully.	Security – Mandatory

92 2.15 Interoperability Testing

- 93 Tests in this section attempt to use a variety of dual interface production PIV and PIV-I cards in the
- 94 system. The FICAM Testing Program will vary the selection of cards on an as needed basis.

95 2.16 Cryptographic Testing

- 96 Tests in this section attempt to confirm the solution's ability to handle all required cryptographic
- 97 algorithms as specified in the Federal PKI Common Policy and NIST SP800-78-3.

Test	Components	Description	Test condition	Туре
2.16.1RSA PKCS#1 v1.5 (1024)	V	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	NIST card#7 registers successfully.	Security – Mandatory
2.16.2RSA PKCS#1 v1.5 (2048)	V	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 registers successfully.	Security – Mandatory

Test	Components	Description	Test condition	Туре
2.16.3RSA PKCS#1 v1.5 (3072)	V	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	TBD	Security – Mandatory
2.16.4RSASSA-PSS (1024)	V	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	TBD (valid through 1/1/2014)	Security – Mandatory
2.16.5 RSASSA-PSS (2048)	V	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 registers successfully.	Security – Mandatory
2.16.6RSASSA-PSS (3072)	V	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	TBD	Security – Mandatory
2.16.7 RSA key transport (1024)	V		TBD (valid through 1/1/2014)	Security – Mandatory
2.16.8RSA key transport (2048)	V		TBD	Security – Mandatory
2.16.9 RSA key transport (3072)	V		TBD	Security – Mandatory
2.16.10 ECDSA (P- 256)	v	Verify Product's ability to validate signatures using ECDSA (P-256)	NIST card#4 registers successfully.	Security – Mandatory
2.16.11 ECDSA (P-384)	V	Verify Product's ability to validate signatures using ECDSA (P-384)	NIST card#5 registers successfully.	Security – Mandatory
2.16.12 ECDH (P- 256)	V		TBD	Security – Mandatory
2.16.13 ECDH (P- 384)	V		TBD	Security – Mandatory
2.16.14 SHA-1	V	Verify Product's ability to validate signatures using SHA-1	NIST card#7 registers successfully.	Security – Mandatory
2.16.15 SHA-256	V	Verify Product's ability to validate signatures using SHA-256	NIST card#1 registers successfully.	Security – Mandatory
2.16.16 SHA-384	V	Verify Product's ability to validate signatures using SHA-384	NIST card#5 registers successfully.	Security – Mandatory
2.16.17 2TDEA	V	Verify Product's ability for SYM-CAK using 2TDEA	TBD	Security - Optional*

Comment [FICAM1]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM2]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM3]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM4]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM5]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM6]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Test	Components	Description	Test condition	Туре
2.16.18 3TDEA	V	Verify Product's ability for	TBD	Security -
	V	SYM-CAK using 3TDEA		Optional*
2.16.19 AES-128	V	Verify Product's ability for	TBD	Security -
	V	SYM-CAK using AES-128		Optional*
2.16.20 AES-192	V	Verify Product's ability for	TBD	Security -
	V	SYM-CAK using AES-192		Optional*
2.16.21 AES-256		Verify Product's ability for	TBD	Security -
,	V	SYM-CAK using AES-256		Optional*
2.16.22 RSA key		Verify Product's ability to	NIST card#1	
exponent	V	validate signatures using	registers	Security -
65,537	V	RSA PKCS#1 v1.5 (2048)	successfully.	Mandatory
(2^16+1)		w/exponent of 65,537.		
2.16.23 RSA key		Verify Product's ability to	TBD	
exponent	V	validate signatures using		Security -
(2^256-1)	V	RSA PKCS#1 v1.5 (2048)		Optional*
		w/exponent of 2^256-1.		

anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Comment [FICAM7]: Optional SYM-CAK. We

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM8]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM9]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM10]: These could also be tests for variants of TLS to OCSP responders. Would have to develop PKI services for this case for all algorithms.

Comment [FICAM11]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

99

3 Authentication at Time of Access Test Cases

3.1 Signature Verification

- Applications must be able to verify digital signatures on each certificate in the certification path using
- the public key from the previous certificate in the path. These test cases validate signatures in the
- certificates found in the certification path.

Test		Components	Description	Test condition	Туре
	Valid Signature PIV	H, V, R	Verify Product's ability to validate signatures in the certificates found in the certification path for a PIV credential.	Card 1: PIV Golden Receives an access grant Successfully.	Security – Mandatory
	Valid Signatures PIV-I	H, V, R	Verify Product's ability to validate signatures in the certificates found in the certification path for a PIV-I credential.	Card 2: PIV-I Golden Receives an access grant Successfully.	Security – Mandatory
0.1.0	Invalid CA Signature	٧	Verify Product's ability to recognize invalid signature on an intermediate CA in the certification path.	Card 1: (Golden PIV Card) with Path 1 fails to receive an access grant.	Security – Mandatory
0	Invalid End Entity	V	Verify Product's ability to recognize invalid signature on the End Entity certificate.	Card 5: invalid PIV/Card Auth Signer fails to receive an access grant.	Security – Mandatory

102

110 111

3.2 Certificate Validity Periods

The Product must verify notBefore time of each certificate to be earlier than or equal to the current time. The Product must also verify notAfter to time be to be later or equal to the current time. The following tests validate notBefore and notAfter values in each certificate in the path.

Test	Components	Description	Test condition	Туре
3.2.1 Invalid CA notBefore Date	V	Verify Product's ability to reject a credential when notBefore date of the intermediate CA certificate is sometime in the future.	Card 1: (Golden PIV Card) fails access grant with Path 2.	Security – Mandatory
3.2.2 Invalid End Entity certificate notBefore Date	V	Verify Product's ability to reject a credential when notBefore date of the End Entity certificate is sometime in the future.	Card 12: (Certs not yet valid) access grant fails.	Security – Mandatory
3.2.3 Invalid CA notAfter Da	te V	Verify Product's ability to reject a credential when notAfter date of the intermediate certificate is sometime in the past.	Card 1: (Golden PIV Card) fails access grant with Path 3.	Security – Mandatory
3.2.4 Invalid End Entity certificate notAfter Da	V	Verify Product's ability to reject a credential when notAfter date of the End Entity certificate is sometime in the past.	Card 13: (Certs Expired) access grant fails.	Security – Mandatory

3.3 Name Chaining

113 The purpose of the following test is to verify the Product's ability to check that names chain correctly 114 within the certification path.

Test	Components	Description	Test condition	Туре
3.3.1 Invalid Name Chaining End Entity Certificate	V	Verify Product's ability to reject a credential when common name portion of the of the issuer's name in the End Entity certificate does not match common name portion of subject's name in the previous intermediate certificate.	Card 1: (Golden PIV Card) fails access grant with Path 4.	Security – Mandatory

119 120

3.4 Basic Constraints Verification

118 Test in this section are used to verify that the Product correctly processes **basicConstraints** extension.

Test	Components	Description	Test condition	Туре
3.4.1 Invalid Missing Basic Constraints	V	Verify Product's ability to recognize when the intermediate CA certificate is missing basicConstraints extension.	Card 1: (Golden PIV Card) fails access grant with Path 5.	Security – Mandatory
3.4.2 Invalid CA False Critical	V	Verify Product's ability to recognize when the basicConstraints extension is present and critical in the intermediate CA certificate but the CA component is false.	Card 1: (Golden PIV Card) fails access grant with Path 6.	Security – Optional
3.4.3 Invalid CA False not Critical	V	Verify Product's ability to recognize when the basicConstraints extension is present and not critical in the intermediate CA certificate but the CA component is false.	Card 1: (Golden PIV Card) fails access grant with Path 7.	Security – Optional
3.4.4 Invalid pathLenConst raint	V	Verify Product's ability to recognize when the first certificate in the path includes basicConstraints extension with a pathLenConstraint of 0 (this prevents additional intermediate certificates from appearing in the path). The first certificate is followed by the second intermediate CA certificate and an End Entity certificate.	Card 1: (Golden PIV Card) fails access grant with Path 8.	Security – Mandatory

121 3.5 Key Usage Verification

122

124 125 Tests in this section verify the Product's ability to correctly process keyUsage extension in a certificate

when subject public key is to be used to verify signatures on certificates and CRLs.

Test		Components	Description	Test condition	Туре
3.5.1	Invalid keyUsage Critical keyCertSign False	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which keyCertSign is false.	Card 1: (Golden PIV Card) fails access grant with Path 9.	Security – Mandatory
3.5.2	Valid keyUsage Not Critical	V	Verify Product's ability to recognize when the intermediate certificate includes a non-critical keyUsage extension.	Card 1: (Golden PIV Card) fails access grant with Path 10.	Security – Mandatory
3.5.3	Invalid keyUsage Critical cRLSign False	V	Verify Product's ability to recognize when the intermediate certificate includes a critical keyUsage extension in which cRLSign is false.	Card 1: (Golden PIV Card) fails access grant with Path 11.	Security – Mandatory

3.6 Certificate Policies

126

127 Tests in this section verify the Product's ability to correctly process **certificatePolicies** extension.

Test		Components	Description	Test condition	Туре
			7		
3.6.1	Explicit		With the trust anchor set	Production PIV-I	
	Certificate		to Commercial Root check	receives access	
	Policy		to see if the validation	grant.	
	Required and		software is able to		
	Present	V	recognize when an		Security –
		-	explicit certificate policy is		Mandatory
			required and present in		
			the certificate path. The		
			explicit policy will be set		
			to PIV-I Hardware.		
3.6.2	Explicit		With the trust anchor set	Production PIV-I	
	Certificate		to Commercial Root check	receives access	
	Policy		to see if the validation	denied.	
	Required and		software is able to)
	not Present		recognize when an		
		V	explicit certificate policy is required and not present		Security –
		V	in the certificate path.		Mandatory
			The explicit policy will be		
			set to an arbitrary value		
			that is not present in the		
			certificate path (e.g., OID		
			value 1.2.3.4).		
3.6.3	Explicit		With the trust anchor set	Production PIV-I	
	Certificate		so the certificate path	receives access	
	Policy		requires trust across the	grant.	
	Required		Commercial Bridge to		
	Across Bridge		Federal Common Policy		
	and Present		CA, check to see if the		
	in End Entity		validation software is able		
	Certificate		to recognize when an		Security –
		V	explicit certificate policy is		Mandatory
			required and present in		ivialidatory
			the certificate in a		
			bridged trust		
			environment. The explicit		
			policy will be set to PIV-I		
			Hardware.		
			Test Condition:		
			production PIV-I passes.		

Test	Components	Description	Test condition	Туре
3.6.4 Explicit Certificate Policy Required Across Bridge and not Present in End Entity Certificate	V	With the trust anchor set so the certificate path requires trust across the Commercial Bridge to Federal Common Policy CA, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate in a bridged trust environment. The explicit policy will be set to an arbitrary value that is not present in the certificate chain (e.g., OID value 1.2.3.4).	Production PIV-I receives access denied.	Security – Mandatory
3.6.5 Explicit Certificate Policy Required Across Bridge and Present in Path, but not Present in End Entity Certificate	V	With Federal Common Policy CA trust anchor, check to see if the validation software is able to recognize when an explicit certificate policy is required and not present in the certificate — however, is present somewhere in the certificate path. The explicit policy will be set to a value that is present in the certificate path, but does not map to the end entity certificate (e.g., High Hardware).	Production PIV-I receives access denied.	Security – Mandatory

3.7 Inhibit Policy Mappings

- 131 The test in this section verifies the application's ability to process the inihibitPolicyMapping field of the
- 132 **policyConstraints** extension and to verify that policy mappings are processed correctly after policy
- mapping has been inhibited.

Test	Components	Description	Test condition	Туре
3.7.1 Invalid inhibitPolicyM apping	V	The first intermediate certificate asserts NIST-test-policy-1 and includes a policyConstraints extension with inhibitPolicyMapping set to 0. The second intermediate certificate asserts Policy A and maps Policy A to Policy B. The end entity certificate asserts Policy A and Policy B.	Card 1: (Golden PIV Card) fails access grant with Path 12.	Security – Mandatory

3.8 Name Constraints

134

135 Tests in this section verify the Product's ability to correctly process nameConstraints extension.

Test		Components	Description	Test condition	Туре
3.8.1	Valid DN nameConstrai nts	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree.	Card 1: (PIV Golden) access grant succeeds.	Security – Mandatory
3.8.2	Invalid DN nameConstrai nts	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls outside that subtree.	Card 1: (Golden PIV Card) fails access grant with Path 13.	Security – Mandatory

Test	Components	Description	Test condition	Туре
3.8.3 Invalid DN nameConstrai nts invalid SAN	V	The system recognizes when the intermediate certificate includes a nameConstraints extension that specifies a single permitted subtree. The end entity certificate includes a subject name that falls within that subtree and subjectAltName with a DN that falls outside that subtree.	Card 1: (Golden PIV Card) fails access grant with Path 14.	Security – Mandatory

3.9 Certificate Revocation Tests (CRL)

Tests in this section verify the Product's ability to retrieve and process valid revocation data for each

138 certificate in the path via CRL.

Test	Components	Description	Test condition	Туре
3.9.1 Unavailable CRL	V	The system recognizes when no revocation information is available for the End Entity certificate.	Card 1: (Golden PIV Card) fails access grant with Path 15.	Security – Mandatory
3.9.2 Revoked CA	V	The system recognizes when a second intermediate CA certificate is revoked.	Card 1: (Golden PIV Card) fails access grant with Path 16.	Security – Mandatory
3.9.3 Revoked End Entity	V	The system recognizes when the End Entity certificate is revoked.	Card 24: Revoked status.	Security – Mandatory
3.9.4 Invalid CRL Signature	V	The system recognizes when the CRL has an invalid signature	Card 1: (Golden PIV Card) fails access grant with Path 17	Security – Mandatory
3.9.5 Invalid CRL Issuer Name	V	The system recognizes when a certificate in the path links to a CRL issued by a CA other than that which issued the certificate.	Card 1: (Golden PIV Card) fails access grant with Path 18.	Security – Mandatory
3.9.6 Old CRL nextUpdate	V	The system recognizes when a certificate in the path has an expired nextUpdate value.	Card 1: (Golden PIV Card) fails access grant with Path 19.	(Security – Mandatory)

Test	Components	Description	Test condition	Туре
3.9.7 Invalid notBefore Date	v	The system recognizes when a certificate in the path points to a CRL with a notBefore Date in the future.	Card 1: (Golden PIV Card) fails access grant with Path 20.	Security – Mandatory
3.9.8 Invalid Distribution Point	V	The system recognizes when a certificate in the path has an incorrect distribution point.	Card 1: (Golden PIV Card) fails access grant with Path 21.	Security – Mandatory

139 3.10 CHUID Verification

141 142

140 Tests in this section verify the system's ability to correctly verify CHUID's validity.

i				
Test	Components	Description	Test condition	Туре
3.10.1Invalid CHUID signature	V	The system recognizes when the CHUID signature is invalid and does not verify.	Card 4: (Invalid CHUID Signature) fails access grant.	Security – Mandatory
3.10.2Expired CHUID signer	V	The system recognizes when the CHUID signer certificate is expired.	Card 9: (Expired CHUID signer) fails access grant.	Security – Mandatory
3.10.3Expired CHUID	V	The system recognizes when the CHUID is expired.	Card 14: (Card Expired) fails access grant.	Security – Mandatory
3.10.4FASC-N != in CHUID	v	The system recognizes when the FASC-N in the CHUID does not equal the FASC-N in the PIV Auth Cert.	Card 15: (FASC-N in CHUID !=) fails access grant.	Security – Mandatory
3.10.5UUID != in CHUID	V	The system recognizes when the UUID in the CHUID does not equal the UUID in the PIV Auth Cert.	Card 19: (UUID in CHUID !=) fails access grant.	Security – Mandatory

143 3.11 Facial Image Verification

144

147

The test in this section verifies the Product's ability to correctly verify Facial Image object. Test cards

use CHUID Signer Certificate for biometric objects.

Test	Components	Description	Test condition	Туре
3.11.1Invalid Facial Image signature	V	The system recognizes when the Facial Image signature is invalid and does not verify.	Card 6: (bad photo signature) access grant fails.	Security – Optional

146 3.12 FINGERPRINT Verification

Tests in this section verify the Product's ability to correctly verify FINGERPRINT object. Test cards use

148 CHUID Signer Certificate for biometric objects.

Test	Components	Description	Test condition	Туре
3.12.1 Invalid Fingerprint signature	V	The system recognizes when the Fingerprint signature is invalid and does not verify.	Card 7: (bad fingerprint signature) access grant fails.	Security – Mandatory
3.12.2Valid Bio	H, V, R	With fingerprint checking enabled, a good credential is presented to the system with a valid fingerprint.	PIV-I access grant succeeds.	Security – Mandatory
3.12.3 Invalid Bio	H, V, R	With fingerprint checking enabled, a good credential is presented to the system with an invalid fingerprint.	PIV-I access grant fails.	Security – Mandatory

3.13 Security Object Verification

150 The test in this section verifies the Product's ability to correctly verify Security Object.

Test	Components	Description	Test condition	Туре
3.13.1 Invalid Security Object signature	V	The system recognizes when the Security Object signature is invalid and does not verify.	Card 8: (bad security object signature) access grant fails.	Security – Optional

153 3.14 OCSP Response Checking

154 Tests in this section verify the Product's ability to validate OCSP responses.

Test	Components	Description	Test condition	Туре
3.14.1Good OCSP Signer	V	The system successfully validates a good credential using an OCSP response with a good signature.	Card 1: Golden PIV is granted access.	Security – Mandatory
3.14.2 Expired OCSP Signer	V	Validation fails using an OCSP response with an expired signature for a good card.	Card 1: Golden PIV access is denied.	Security – Mandatory
3.14.3 Revoked OCSP Signer with PKIX_OCSP_N OCHECK present	V	Validation succeeds using an OCSP response with a revoked signature for a good card with PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV is granted access.	Security – Mandatory
3.14.4 Revoked OCSP Signer with PKIX_OCSP_N OCHECK not present	V	Validation fails using an OCSP response with a revoked signature for a good card without PKIX_OCSP_NOCHECK present.	Card 1: Golden PIV access is denied.	Security – Mandatory
3.14.5 Invalid OCSP Signer	V	Validation fails using an OCSP response with an malformed signature for a good card.	Card 1: Golden PIV access is denied	Security – Mandatory

155 3.15 Interoperability Testing

- 156 Tests in this section attempt to use a variety of dual interface production PIV and PIV-I cards in the
- 157 system. The FICAM Testing Program will vary the selection of cards on an as needed basis.

158 3.16 Cryptographic Testing

- 159 Tests in this section attempt to confirm the solution's ability to handle all required cryptographic
- algorithms as specified in the Federal PKI Common Policy and NIST SP800-78-3.

Test	Components	Description	Test condition	Туре
3.16.1RSA PKCS#1 v1.5 (1024)	V	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (1024).	NIST card#7 access is granted.	Security – Mandatory
3.16.2RSA PKCS#1 v1.5 (2048)	V	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (2048).	NIST card#1 access is granted.	Security – Mandatory

v0.1.0

Test	Components	Description	Test condition	Туре
3.16.3RSA PKCS#1 v1.5 (3072)	V	Verify Product's ability to validate signatures using RSA PKCS#1 v1.5 (3072).	TBD	Security – Mandatory
3.16.4RSASSA-PSS (1024)	V	Verify Product's ability to validate signatures using RSASSA-PSS (1024).	TBD (valid through 1/1/2014)	Security – Mandatory
3.16.5 RSASSA-PSS (2048)	V	Verify Product's ability to validate signatures using RSASSA-PSS (2048).	NIST card#2 access is granted.	Security – Mandatory
3.16.6RSASSA-PSS (3072)	V	Verify Product's ability to validate signatures using RSASSA-PSS (3072).	TBD	Security – Mandatory
3.16.7 RSA key transport (1024)	V		TBD (valid through 1/1/2014)	Security – Mandatory
3.16.8 RSA key transport (2048)	V		TBD	Security – Mandatory
3.16.9 RSA key transport (3072)	V		TBD	Security – Mandatory
3.16.10 ECDSA (P- 256)	V	Verify Product's ability to validate signatures using ECDSA (P-256)	NIST card#4 access is granted.	Security – Mandatory
3.16.11 ECDSA (P-384)	V	Verify Product's ability to validate signatures using ECDSA (P-384)	NIST card#5 access is granted in CHUID mode. TBD for PIV Auth.	Security – Mandatory
3.16.12 ECDH (P- 256)	V		TBD	Security – Mandatory
3.16.13 ECDH (P- 384)	V		TBD	Security – Mandatory
3.16.14 SHA-1	v	Verify Product's ability to validate signatures using SHA-1	NIST card#7 access is granted.	Security – Mandatory
3.16.15 SHA-256	V	Verify Product's ability to validate signatures using SHA-256	NIST card#1 access is granted.	Security – Mandatory
3.16.16 SHA-384	V	Verify Product's ability to validate signatures using SHA-384	NIST card#5 access is granted.	Security – Mandatory
3.16.17 2TDEA	V	Verify Product's ability for SYM-CAK using 2TDEA	TBD	Security - Optional*
3.16.18 3TDEA	V	Verify Product's ability for SYM-CAK using 3TDEA	TBD	Security - Optional*

Comment [FICAM12]: Drop this requirement. In PACS, nothing encrypts to the card/person yet.

Comment [FICAM13]: Drop this requirement. In PACS, nothing encrypts to the card/person yet.

Comment [FICAM14]: Drop this requirement. In PACS, nothing encrypts to the card/person yet.

Comment [FICAM15]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM16]: We anticipate dropping this requirement as we are unaware of industry solutions that use the KMK for PACS. Are there live use cases for this key?

Comment [FICAM17]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM18]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Test	Components	Description	Test condition	Туре
3.16.19 AES-128	V	Verify Product's ability for	TBD	Security -
	V	SYM-CAK using AES-128		Optional*
3.16.20 AES-192	V	Verify Product's ability for	TBD	Security -
	V	SYM-CAK using AES-192		Optional*
3.16.21 AES-256	V	Verify Product's ability for	TBD	Security -
	V	SYM-CAK using AES-256		Optional*
3.16.22 RSA key		Verify Product's ability to	NIST card#1 access	
exponent	V	validate signatures using	is granted.	Security -
65,537	V	RSA PKCS#1 v1.5 (2048)		Mandatory
(2^16+1)		w/exponent of 65,537.		
3.16.23 RSA key		Verify Product's ability to	TBD	
exponent	V	validate signatures using		Security -
(2^256-1)	V	RSA PKCS#1 v1.5 (2048)		Optional*
		w/exponent of 2^256-1.		

Comment [FICAM19]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM20]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

Comment [FICAM21]: Optional SYM-CAK. We anticipate dropping this requirement as we are unaware of interoperable solutions from industry that leverage SYM-CAK. Are there live interoperable solutions using this key?

Could also be used in TLS between infrastructure components. Is this done today?

162

163

166 167

3.17 Continuity of Operations Testing

Tests in this section prove that the system can recover from a variety of environment conditions that could result in the loss of availability of service.

Test	Components	Description	Test condition	Туре
3.17.1 Network Connectivity Loss to Panel	H, V, R	The network connection is dropped to all boards within a panel.	Get an access grant at door with Test Card 1: PIV Golden. Disconnect network cables from panel and reattempt access with Test Card 1: PIV Golden. Access should be granted.	Usability - Optional
3.17.2 Network Connectivity Loss to Server	H, V, R	The network connection is dropped from the server(s).	Get an access grant at door with Test Card 1: PIV Golden. Disconnect network cable(s) from server(s) and reattempt access with Test Card 1: PIV Golden. Access should be granted.	Usability - Optional
3.17.3Services Stopped on Server	H, V, R	The services have stopped on the server.	Get an access grant at door with Test Card 1: PIV Golden. Manually stop any service associated with the PACS on the server(s) and reattempt access with Test Card 1: PIV Golden. Access should be granted.	Usability - Optional

Test	Components	Description	Test condition	Туре
3.17.4 Power Loss to Panel	H, V, R	A/C Power loss to panel.	Get an access grant at door with Test Card 1: PIV Golden. Abruptly remove all power sources from the power supply. Restore power, and reattempt access with Test Card 1: PIV Golden. Access should be granted.	Usability - Optional



169 4 PACS Design Use Cases

4.1 Security Boundaries

170

4.1 Security Boundaries				
Test	Components	Description	Test condition	Туре
4.1.1 Attack side processing 1	н, v, п	"all security relevant processing shall be performed on the secure side of the door." No security relevant decisions shall be made by system components that do not belong to the cardholder's credential when they are on the attack side of the door.	Confirm door controllers, head- end are capable of being located on the safe side of perimeter.	Security – Mandatory
4.1.2 Attack side processing 2	H, V, R	"door reader shall be a transparent reader".	Confirm physical inspection and design documentation.	Security – Mandatory
4.1.3 Attack side processing 3	H, V, R	"compensating controls applied such as tamper switches and FIPS 140-2 certified cryptographic processing within the reader itself. Specific waivers shall be granted on a per implementation basis for Approved Products List (APL) approved compensating controls".	Document all supplemental security devices and check against APLs, FIPS 140-2.	Security – Optional

4.2 Registering Physical Access Privileges

Test	<i>8 8</i>	Components	Description	Test condition	Туре
1630		Components	Description	rest condition	Турс
4.2.1	Populations 1	Н	 shall support, at a minimum, three specific groups: guests, visitors and regular access" shall be able to define: User populations: Guests, Visitors, Regular Access 	Confirm physical inspection and design documentation.	Usability - Optional
4.2.2	Populations 2	Н	shall be able to define: Access points for each population.	Verify by system design review.	Usability - Optional
4.2.3	Populations 3	Н	shall be able to define: Temporal access rules for each population.	Verify by system design review.	Usability - Optional
4.2.4	Populations 4	V	 shall be able to define: Challenge and verification program for each population shall be able to define: Authentication approach for each population and each zone/point of access in accord with NIST SP 800-116. 	Verify by system design review.	Usability - Optional
4.2.5	Valid Registration	v	No credential shall be registered for which there is no valid trust path per the relying party PKI policy.	Derive from the overall results of the PKI Use Cases found in section 2.	Security – Mandatory
4.2.6	Valid Registration 2	Н, V	The system shall allow for integrated provisioning once a positive determination of a credential's suitability has been made.	Verify automated registration process for PIV credentials.	Usability - Optional

Test	Components	Description	Test condition	Туре
4.2.7 Valid Registration 3	Н, V	The system shall allow for integrated provisioning once a positive determination of a credential's suitability has been made.	Verify automated registration process for all credentials.	Usability - Optional
4.2.8 Binding to Bearer 1	H, V, R	shall provide access grant functionality to evaluate credentials to determine binding with the bearer.	Use logs to verify that attempt to receive an access grant a good card with a correct biometric succeed, and attempts using an incorrect and improperly signed biometric fail.	Usability - Optional
4.2.9 Binding to Bearer 2	H, V	shall provide the means to select which biometrics are used to link bearer to credential.	Confirm multiple factors can be configured for access grant station.	Usability - Optional
4.2.10 Policy Constraints	V	shall provide the means to select which x.509 constraints are evaluated such as policy constraints, name constraints and key usage. This configuration will reflect the customer's PKI relying party policy.	Verify configurability of the path determination and validation component of the Product.	Usability - Optional
4.2.11 Workflow	H, V	Workflow shall include sponsor approval and security administrator approval; No credential shall be granted authorization privileges to a Trusted PACS without approval.	Confirm system design workflow. An administrative password must be utilized for system changes and enrollment.	Usability - Optional

176 4.3 Validation at Time of Access

T	T.5 Valuation at Time of Access					
Test		Components	Description	Test condition	Туре	
4.3.1	Signed CHUID	H, V, R	shall support: signed CHUID.	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	Usability - Optional	
4.3.2	Card Authenticatio n Key	H, V, R	shall support: Card Authentication Key.	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	Usability - Optional	
4.3.3	PIV Authenticatio n Key + PIN	H, V, R	shall support: PIV Authentication Key + PIN.	Use Authentication Test logs to verify that all good cards were allowed access at the door reader.	Usability - Optional	
4.3.4	PIV Authenticatio n Key + PIN + BIO	H, V, R	shall support: PIV Authentication Key + PIN + BIO.	Use Authentication Test logs to verify that all good cards with valid BIO available were allowed access at the door reader.	Usability - Optional	
4.3.5	PIN to PACS	H, V	May support PIN to PACS secondary to other authentication mode.	If PIN to PACS available, verify that it must be tied to another authentication mode.	Usability - Optional	

179 4.4 Portal Hardware

Test		Description	Test condition	Typo
rest	Components	Description	rest condition	Туре
4.4.1 Readers 1	H, V, R	Where multiple authentication modes are supported, readers shall support bidirectional communications with the system.	Confirmed using protocol sniffing, review of logs produced during authentication testing.	Security – Mandatory
4.4.2 Readers 2	H, V, R	For multi-factor readers, applicant's system must allow modification of an individual reader or groups of readers' authentication mode from the server or a client/workstation to the server.	Verify by system design review.	Usability - Optional
4.4.3 Readers 3	H, V, R	For multi-factor readers, the site administrator arbitrarily decides that all readers or a subset of readers must require either more or fewer authentication factors than the readers are presently configured for.	Verify by system design review.	Usability - Optional
4.4.4 Readers 4	H, V, R	For multi-factor readers, based on temporal access rules the administrator set, the system should support dynamic assignment of individuals (or groups of individuals) and resources (doors) on a time based schedule.	Verify by system design review.	Usability - Optional

Test	Components	Description	Test condition	Туре
4.4.5 Readers 5	H, V, R	For multi-factor readers, based on FPCON, MARCON or other similar structured emergency response protocol for which the vendor claims support, in no case shall there be a requirement for an administrator's physical presence at a reader be considered compliant.	Verify by system design review.	Usability - Optional
4.4.6 Readers 6	H, V, R	For multi-factor readers, if a time delay of longer than 120 seconds is required for a reader to change modes, this too shall be considered noncompliant.	Verify by system design review.	Usability - Optional

4.5 Auditing and Logging

Test	Components	Description	Test condition	Туре
4.5.1 Auditing 1	H, V	Verify by system design	Verify by review of	Security –
	1.,, 1	review.	logs and reports.	Mandatory
4.5.2 Auditing 2		Granularity of auditing	Verify by review of	
		records shall be to the	logs and reports.	
		card and individual		
	H, V	transaction. These shall		Security –
	11, V	be easily verifiable		Mandatory
		through a reporting tool		
		or any other log and audit		
		viewing capability.		
4.5.3 Auditing 3		The Product shall provide	Verify by review of	
		auditing/logging of all PKI	logs and reports.	
		processing to include:		
		 Nonce generation 		Coousitu
	V	 Challenges 		Security –
		 Responses 		Mandatory
		• PDVAL		
		 Revocation status 		
		checking.		

Test	Components	Description	Test condition	Туре
4.5.4 Auditing 4	н, ∨	The Product shall provide auditing/logging of credential number processing and transmission.	Verify by review of logs and reports.	Security – Mandatory
4.5.5 Auditing 5	н, v	The Product shall provide auditing/logging of all software driven configuration changes.	Verify by review of logs and reports.	Security – Mandatory
4.5.6 Auditing 6	V	The Product shall provide auditing/logging of periodic certificate PDVAL and status checking.	Verify by review of logs and reports.	Security – Mandatory
4.5.7 Auditing 7	н, v	The Product shall provide auditing/logging of Card activity (e.g., 3 days of card activity).	Verify by review of logs and reports.	Security – Mandatory
4.5.8 Auditing 8	н, V	The Product shall provide auditing/logging of a card's whereabouts in system.	Verify by review of logs and reports.	Security – Mandatory
4.5.9 Auditing 9	v	The Product shall provide auditing/logging of PKI policies for name constraints, path constraints, validity checks.	Verify by review of logs and reports.	Security – Mandatory
4.5.10 Auditing 10	н	The Product shall provide auditing/logging of individual and group reporting of alarms (e.g., door force, door prop).	Verify by review of logs and reports.	Security – Mandatory
4.5.11Auditing 11	H, V	The Product shall provide auditing/logging of what date individuals were provisioned or deprovisioned and by whom.	Verify by review of logs and reports.	Security – Mandatory
4.5.12 Auditing 12	Н, V	The Product shall provide auditing/logging of all readers and their modes.	Verify by review of logs and reports.	Security – Mandatory
4.5.13 Auditing 13	н, ∨	The Product shall provide auditing/logging of configuration download status to system components.	Verify by review of logs and reports.	Security – Mandatory

4.6 Security Certification and Accreditation

Test	Interface	Description	Test condition	Туре
4.6.1 UL Assessment	H, V	Each component in the system shall have, at a minimum, a UL 249 listing.	Verify UL listing.	Usability - Optional
4.6.2 FIPS 201-1	H, V, R	Each component in the system shall have GSA FIPS-201-1 APL status, as applicable.	Verify APL listing.	Usability - Optional
4.6.3 FIPS 140-2	H, V, R	Each component in the system shall have FIPS 140-2 certification, as applicable.	Verify APL listing.	Security – Mandatory

182 4.7 Biometric in PACS

Test	Interface	Description	Test condition	Туре
4.7.1 Biome Encry	H, V, R	Biometric identifiers shall be encrypted at rest and in transmission throughout the system.	Verify by system design and inspection of database.	Security – Mandatory

4.8 Operational Controls

Test	Interface	Description	Test condition	Туре
4.8.1 System Configuration	H, V, R	The system shall have the ability to manage the system through software controlled configuration management methods. Initial configuration of hardware settings (e.g., DIP switches) is allowed at installation only and not for management of the hardware tree.	Verify by use of the system.	Usability - Optional
4.8.2 Component Addressing	H, V, R	Each physical component shall be separately defined and addressable within the server user interface.	Verify by setting up of system.	Usability - Optional
4.8.3 Configuration Downloads	H, V, R	The system shall support configuration downloads to each component.	Verify by setting up of system.	Usability - Optional