3.10 Test PIV Card 10

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

FASC-N: D650185A0D412D5AB49915A16CDA75257286D6B086501843E2
(Agency Code = 3201, System Code = 1624, Credential Number = 556438,
CS=1, ICI=3, PI=9545326551, OC=1, OI=3201, POA=1)
GUID: all 0x00
Expiration Date: 20301231
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

PIV Authentication Certificate: PIV Test Card 10: PIV Authentication Certificate

Card Authentication Certificate: PIV Test Card 10: Card Authentication Certificate

Digital Signature Certificate: PIV Test Card 10: Digital Signature Certificate

Key Management Certificate: PIV Test Card 10: Key Management Certificate

Cardholder Fingerprints:

dummy fingerprints, RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Security Object: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Cardholder Facial Image: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Printed Information:

Name: Test Cardholder X
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012354
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 4
offCardCertURL:
http://smime2.nist.gov/525B544F232C097BB3840ED51B97EB028156D3AFBFFEFF4BFB38A4FDB0112053

key reference 82: PIV Test Card 10: Retired Key Management Key E
Certificate Tag 5FC10D: PIV Test Card 10: Retired Key Management Certificate E

key reference 92: PIV Test Card 10: Retired Key Management Key D

key reference 93: PIV Test Card 10: Retired Key Management Key C

key reference 94: PIV Test Card 10: Retired Key Management Key A

key reference 95: PIV Test Card 10: Retired Key Management Key B

Cardholder Iris Images: Not present

3.11 Test PIV Card 11

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

FASC-N: D6501858289D6DCACC9325A16859A46927C9D45C86501843E2
(Agency Code = 3201, System Code = 0295, Credential Number = 759494,
CS=1, ICI=1, PI=6464979587, OC=1, OI=3201, POA=1)
GUID: all 0x00
Expiration Date: 20301001
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1, but with some bits in signature block changed.

PIV Authentication Certificate: PIV Test Card 11: PIV Authentication Certificate, GZIP compressed

Card Authentication Certificate: PIV Test Card 11: Card Authentication Certificate, GZIP compressed

Digital Signature Certificate: PIV Test Card 11: Digital Signature Certificate, GZIP compressed

Key Management Certificate: PIV Test Card 11: Key Management Certificate, GZIP compressed

Cardholder Fingerprints: dummy fingerprints

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1, but with some bits in signature block changed.

Security Object:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1, but with some bits in signature block changed.

Cardholder Facial Image:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1, but with some bits in signature block changed.

Printed Information:

Name: Test Cardholder
Employee Affiliation: Employee
Expiration date: 20301001 (2030OCT01)
Agency Card Serial Number: 0170336744
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object: Not present

Cardholder Iris Images: Not present

3.12 Test PIV Card 12

Use the following FASC-N in Cardholder Fingerprints and Cardholder Facial Image:

FASC-N: D650185AB06F2D0811010DA16858810C3352203586501843EB
(Agency Code = 3201, System Code = 5167, Credential Number = 114200,
CS=1, ICI=1, PI=4001354205, OC=1, OI=3201, POA=1)

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

Copy CHUID data object from Test PIV Card 1

PIV Authentication Certificate:

PIV Test Card 12: PIV Authentication Certificate, GZIP compressed

Card Authentication Certificate:

PIV Test Card 12: Card Authentication Certificate, GZIP compressed

Digital Signature Certificate:

PIV Test Card 12: Digital Signature Certificate, GZIP compressed

Key Management Certificate:

PIV Test Card 12: Key Management Certificate, GZIP compressed

Cardholder Fingerprints:

dummy fingerprints

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Security Object:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Cardholder Facial Image:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Printed Information:

Name: Test Cardholder XII
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012355
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object: Not present

Cardholder Iris Images: Not present

3.13 Test PIV Card 13

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

FASC-N: D6501859019B6D0E708DADA168585324D042221586501843EB
(Agency Code = 3201, System Code = 2096, Credential Number = 177465,
CS=1, ICI=1, PI=8949244215, OC=1, OI=3201, POA=1)
GUID: all 0x00
Expiration Date: 20301231
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

PIV Authentication Certificate:

PIV Test Card 13: PIV Authentication Certificate

Card Authentication Certificate:

PIV Test Card 13: Card Authentication Certificate

Digital Signature Certificate:

PIV Test Card 13: Digital Signature Certificate

Key Management Certificate:

PIV Test Card 13: Key Management Certificate

Cardholder Fingerprints:

dummy fingerprints

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Security Object:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Cardholder Facial Image:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

Printed Information:

Name: Test Cardholder XIII
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012356
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object: Not present

Cardholder Iris Images: Not present

3.14 Test PIV Card 14

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

FASC-N: D6501858999CED9992049DA16AD9A19C279A844486501843F5
(Agency Code = 3201, System Code = 4399, Credential Number = 394149,
CS=1, ICI=5, PI=6091935084, OC=1, OI=3201, POA=1)
GUID: all 0x00
Expiration Date: 20301231
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 5

PIV Authentication Certificate: PIV Test Card 14: PIV Authentication Certificate, GZIP compressed

Card Authentication Certificate: PIV Test Card 14: Card Authentication Certificate, GZIP compressed

Digital Signature Certificate: PIV Test Card 14: Digital Signature Certificate, GZIP compressed

Key Management Certificate: PIV Test Card 14: Key Management Certificate, GZIP compressed

Cardholder Fingerprints:

dummy fingerprints

RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 5

Security Object: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 5

Cardholder Facial Image: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 5

Printed Information:

Name: Test Cardholder XIV
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012357
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 4, *offCardCertURL*:
http://smime2.nist.gov/D4746E140242D1786EA2FB41337D65391CECAAB8D6DDCC2E47CF01F42567A801

key reference 82: PIV Test Card 14: Retired Key Management Key E
Certificate Tag 5FC10D: PIV Test Card 14: Retired Key Management Certificate E, GZIP compressed

key reference 92: PIV Test Card 14: Retired Key Management Key D

key reference 93: PIV Test Card 14: Retired Key Management Key C

key reference 94: PIV Test Card 14: Retired Key Management Key B

key reference 95: PIV Test Card 14: Retired Key Management Key A

Cardholder Iris Images: Not present

3.15 Test PIV Card 15

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

FASC-N: D65018591C422CD9E51C6DA1625B88241A49E5A486501843E7
(Agency Code = 3201, System Code = 2722, Credential Number = 693276,
CS=1, ICI=4, PI=7241649364, OC=1, OI=3201, POA=1)
GUID: all 0x00
Expiration Date: 20301231
Asymmetric signature: ECDSA, signed by PIV Content Signer 3

PIV Authentication Certificate: PIV Test Card 15: PIV Authentication Certificate

Card Authentication Certificate: PIV Test Card 15: Card Authentication Certificate

Digital Signature Certificate: PIV Test Card 15: Digital Signature Certificate

Key Management Certificate: PIV Test Card 15: Key Management Certificate

Cardholder Fingerprints:

dummy fingerprints, ECDSA, signed by PIV Content Signer 3

Security Object: ECDSA, signed by PIV Content Signer 3

Cardholder Facial Image: ECDSA, signed by PIV Content Signer 3

Printed Information:

Name: Test Cardholder XV
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012358
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object:

keysWithOnCardCerts = 3, *keysWithOffCardCerts* = 2, *offCardCertURL*:
http://smime2.nist.gov/8B26C59AD929132F405314DD95D8D8243645FC174B7C219D2A9F392E4C52359E

key reference 82: PIV Test Card 15: Retired Key Management Key E
Certificate Tag 5FC10D: PIV Test Card 15: Retired Key Management Certificate E

key reference 83: PIV Test Card 15: Retired Key Management Key C
Certificate Tag 5FC10E: PIV Test Card 15: Retired Key Management Certificate C

key reference 84: PIV Test Card 15: Retired Key Management Key D
Certificate Tag 5FC10F: PIV Test Card 15: Retired Key Management Certificate D

key reference 94: PIV Test Card 15: Retired Key Management Key B

key reference 95: PIV Test Card 15: Retired Key Management Key A

Cardholder Iris Images: Not present

3.16 Test PIV-I Card 16

Card Capability Container:

data model number = 0x10. All other data elements have length value set to zero bytes.

CHUID:

FASC-N: D4E739DA739CED39CE739DA16859B398A798667986501837E8
(Agency Code = 9999, System Code = 9999, Credential Number = 999999,
CS=1, ICI=1, PI=6998931393, OC=1, OI=3201, POA=6)
GUID: 048051b4-2288-41fd-b895-5fe9945e1c63
Expiration Date: 20301231
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV-I Content Signer 1

PIV Authentication Certificate: PIV-I Test Card 16: PIV-I Authentication Certificate

Card Authentication Certificate: PIV-I Test Card 16: Card Authentication Certificate

Digital Signature Certificate: Not present

Key Management Certificate: Not present

Cardholder Fingerprints:

dummy fingerprints

RSA PKCS #1 v1.5 with SHA-256, signed by PIV-I Content Signer 1

Security Object:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV-I Content Signer 1

Cardholder Facial Image:

RSA PKCS #1 v1.5 with SHA-256, signed by PIV-I Content Signer 1

Printed Information:

Name: Test Cardholder XVI
Employee Affiliation: Affiliate
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012359
Issuer Identification: TSTISR320161719

Discovery Object:

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x40 0x00 (no global PIN)

Key History Object: Not present

Cardholder Iris Images: Not present

4 Certificate Details

4.1 CA Certificates

4.1.1 Self-signed Trust Anchor Certificate

serialNumber: 1

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test Trust Anchor for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Trust Anchor for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyCertSign, cRLSign

BasicConstraints (critical): cA = TRUE, pathLenConstraint not present

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectInfoAccess (not critical)

id-ad-caRepository: ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caRepository: http://smime2.nist.gov/PIVTest/CACertsIssuedByTrustAnchor.p7c

4.1.2 RSA 2048 Issuing CA Certificate

Status: not revoked

serialNumber: 2

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test Trust Anchor for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyCertSign, cRLSign

BasicConstraints (critical): cA = TRUE, pathLenConstraint not present

certificatePolicies (not critical):

2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)
2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)
2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)
2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from Self-signed Trust Anchor Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/TrustAnchor.crl

authorityInfoAccess (not critical):

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToTrustAnchor.p7c (certs-only CMS with no certificates)

subjectInfoAccess (not critical):

id-ad-caRepository: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary

id-ad-caRepository: http://smime2.nist.gov/PIVTest/CACertsIssuedByRSA2048CA.p7c (certs-only CMS with no certificates)

4.1.4 ECC P-256 Issuing CA Certificate

Status: not revoked

serialNumber: 4

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test Trust Anchor for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): keyCertSign, cRLSign

BasicConstraints (critical): cA = TRUE, pathLenConstraint not present

certificatePolicies (not critical):

2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)
2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)
2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)
2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from Self-signed Trust Anchor Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/TrustAnchor.crl

authorityInfoAccess (not critical):

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToTrustAnchor.p7c (certs-only CMS with no certificates)

subjectInfoAccess (not critical):

id-ad-caRepository: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary

id-ad-caRepository: http://smime2.nist.gov/PIVTest/CACertsIssuedByECCP-256CA.p7c (certs-only CMS with no certificates)

4.1.6 Expired RSA 2048 Issuing CA Certificate

Status: not revoked

serialNumber: 6

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test Trust Anchor for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 7/23/2005 14:23:35Z, notAfter = 7/23/2010 14:23:35Z

subject: cn=Expired Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyCertSign, cRLSign

BasicConstraints (critical): cA = TRUE, pathLenConstraint not present

certificatePolicies (not critical):

2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)
2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)
2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)
2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from Self-signed Trust Anchor Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/OldTrustAnchor.crl (file does not exist)

authorityInfoAccess (not critical):

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToTrustAnchor.p7c (certs-only CMS with no certificates)

subjectInfoAccess (not critical):

id-ad-caRepository: ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary (directory entry does not exist)

id-ad-caRepository: http://smime2.nist.gov/PIVTest/CACertsIssuedByExpiredRSA2048CA.p7c (file does not exist)

4.1.7 RSA 2048 PIV-I Issuing CA Certificate

Status: not revoked

serialNumber: 7

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test Trust Anchor for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test PIV-I RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyCertSign, cRLSign

BasicConstraints (critical): cA = TRUE, pathLenConstraint not present

certificatePolicies (not critical):

2.16.840.1.101.3.2.1.3.18 (id-fpki-certpcy-pivi-hardware)
2.16.840.1.101.3.2.1.3.19 (id-fpki-certpcy-pivi-cardAuth)
2.16.840.1.101.3.2.1.3.20 (id-fpki-certpcy-pivi-contentSigning)

policyMappings (not critical):

issuerDomainPolicy: 2.16.840.1.101.3.2.1.3.18 (id-fpki-certpcy-pivi-hardware)
subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.71

issuerDomainPolicy: 2.16.840.1.101.3.2.1.3.19 (id-fpki-certpcy-pivi-cardAuth)
subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.72

issuerDomainPolicy: 2.16.840.1.101.3.2.1.3.20 (id-fpki-certpcy-pivi-contentSigning)
subjectDomainPolicy: 2.16.840.1.101.3.2.1.48.73

authorityKeyIdentifier (not critical): SKI from Self-signed Trust Anchor Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/TrustAnchor.crl

authorityInfoAccess (not critical):

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToTrustAnchor.p7c (certs-only CMS with no certificates)

4.2 Content Signer Certificates

4.2.1 PIV Content Signer 1

Status: not revoked

serialNumber: 1

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test PIV Content Signer 1, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical): 2.16.840.1.101.3.6.7 (id-PIV-content-signing)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.2.3 PIV Content Signer 3

Status: not revoked

serialNumber: 3

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test PIV Content Signer 3, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical): 2.16.840.1.101.3.6.7 (id-PIV-content-signing)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.2.5 PIV Content Signer 5

Status: revoked, reason code: key compromise

serialNumber: 5

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test PIV Content Signer 5, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical): 2.16.840.1.101.3.6.7 (id-PIV-content-signing)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.8 (id-fpki-common-devices)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.2.6 PIV-I Content Signer 1

Status: not revoked

serialNumber: 6

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test PIV-I RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test PIV-I Content Signer 1, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.8.7 (id-fpki-pivi-content-signing)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.48.73

authorityKeyIdentifier (not critical): SKI from RSA 2048 PIV-I Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048PIVICA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048PIVICA.p7c

4.13 PIV Test Card 10

4.13.1 PIV Test Card 10: PIV Authentication Certificate

Status: revoked, reason code: key compromise

serialNumber: 1001 (0x3e9)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D650185A0D412D5AB49915A16CDA75257286D6B086501843E2
(Agency Code = 3201, System Code = 1624, Credential Number = 556438, CS=1, ICI=3, PI=9545326551, OC=1, OI=3201, POA=1)
UPN: 32019545326551@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers:
http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.14 PIV Test Card 11

4.14.1 PIV Test Card 11: PIV Authentication Certificate

Status: not revoked

serialNumber: 101 (0x65)

signature: sha256WithRSAEncryption (PKCS #1 v1.5), but with some bits in signature block changed.

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D6501858289D6DCACC9325A16859A46927C9D45C86501843E2
(Agency Code = 3201, System Code = 0295, Credential Number = 759494, CS=1, ICI=1, PI=6464979587, OC=1, OI=3201, POA=1)
UPN: 32015465737401@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers:
http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.14.2 PIV Test Card 11: Card Authentication Certificate

Status: not revoked

serialNumber: 102 (0x66)

signature: sha256WithRSAEncryption (PKCS #1 v1.5), but with some bits in signature block changed.

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: serialNumber=D6501858289D6DCACC9325A16859A46927C9D45C86501843E2, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.6.8 (id-PIV-cardAuth)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D6501858289D6DCACC9325A16859A46927C9D45C86501843E2 (Agency Code = 3201, System Code = 0295, Credential Number = 759494, CS=1, ICI=1, PI=6464979587, OC=1, OI=3201, POA=1)

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.14.3 PIV Test Card 11: Digital Signature Certificate

Status: not revoked

serialNumber: 103 (0x67)

signature: sha256WithRSAEncryption (PKCS #1 v1.5), but with some bits in signature block changed.

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature, nonRepudiation

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.14.4 PIV Test Card 11: Key Management Certificate

Status: not revoked

serialNumber: 104 (0x68)

signature: sha256WithRSAEncryption (PKCS #1 v1.5), but with some bits in signature block changed.

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.15 PIV Test Card 12

4.15.1 PIV Test Card 12: PIV Authentication Certificate

Status: not revoked

serialNumber: 1201 (0x4b1)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D650185AB06F2D0811010DA16858810C3352203586501843EB
(Agency Code = 3201, System Code = 5167, Credential Number = 114200, CS=1, ICI=1, PI=4001354205, OC=1, OI=3201, POA=1)
UPN: 32014001354205@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers:
http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.15.2 PIV Test Card 12: Card Authentication Certificate

Status: not revoked

serialNumber: 1202 (0x4b2)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: serialNumber=D650185AB06F2D0811010DA16858810C3352203586501843EB, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.6.8 (id-PIV-cardAuth)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D650185AB06F2D0811010DA16858810C3352203586501843EB (Agency Code = 3201, System Code = 5167, Credential Number = 114200, CS=1, ICI=1, PI=4001354205, OC=1, OI=3201, POA=1)

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.15.3 PIV Test Card 12: Digital Signature Certificate

Status: not revoked

serialNumber: 1203 (0x4b3)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature, nonRepudiation

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder12@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.15.4 PIV Test Card 12: Key Management Certificate

Status: not revoked

serialNumber: 1204 (0x4b4)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder12@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.16 PIV Test Card 13

4.16.1 PIV Test Card 13: PIV Authentication Certificate

Status: not revoked

serialNumber: 1301 (0x515)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 3/1/2008 08:30:00Z, notAfter = 3/1/2011 08:30:00Z

subject: cn=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D6501859019B6D0E708DADA168585324D042221586501843EB
(Agency Code = 3201, System Code = 2096, Credential Number = 177465, CS=1, ICI=1, PI=8949244215, OC=1, OI=3201, POA=1)
UPN: 32018949244215@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers:
http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.16.2 PIV Test Card 13: Card Authentication Certificate

Status: not revoked

serialNumber: 1302 (0x516)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 3/1/2008 08:30:00Z, notAfter = 3/1/2011 08:30:00Z

subject: serialNumber=D6501859019B6D0E708DADA168585324D042221586501843EB, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.6.8 (id-PIV-cardAuth)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D6501859019B6D0E708DADA168585324D042221586501843EB (Agency Code = 3201, System Code = 2096, Credential Number = 177465, CS=1, ICI=1, PI=8949244215, OC=1, OI=3201, POA=1)

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.16.3 PIV Test Card 13: Digital Signature Certificate

Status: not revoked

serialNumber: 1303 (0x517)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 3/1/2008 08:30:00Z, notAfter = 3/1/2011 08:30:00Z

subject: cn=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature, nonRepudiation

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder13@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.16.4 PIV Test Card 13: Key Management Certificate

Status: not revoked

serialNumber: 1304 (0x518)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 3/1/2008 08:30:00Z, notAfter = 3/1/2011 08:30:00Z

subject: cn=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder13@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.17 PIV Test Card 14

4.17.1 PIV Test Card 14: PIV Authentication Certificate

Status: not revoked

serialNumber: 1401 (0x579)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D6501858999CED9992049DA16AD9A19C279A844486501843F5
(Agency Code = 3201, System Code = 4399, Credential Number = 394149, CS=1, ICI=5, PI=6091935084, OC=1, OI=3201, POA=1)
UPN: 32016091935084@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers:
http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.17.2 PIV Test Card 14: Card Authentication Certificate

Status: not revoked

serialNumber: 1402 (0x57a)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: serialNumber=D6501858999CED9992049DA16AD9A19C279A844486501843F5, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.6.8 (id-PIV-cardAuth)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D6501858999CED9992049DA16AD9A19C279A844486501843F5 (Agency Code = 3201, System Code = 4399, Credential Number = 394149, CS=1, ICI=5, PI=6091935084, OC=1, OI=3201, POA=1)

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.17.3 PIV Test Card 14: Digital Signature Certificate

Status: not revoked

serialNumber: 1403 (0x57b)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature, nonRepudiation

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.17.4 PIV Test Card 14: Key Management Certificate

Status: not revoked

serialNumber: 1404 (0x57c)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.17.5 PIV Test Card 14: Retired Key Management Certificate A

Status: not revoked

serialNumber: 1405 (0x57d)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Expired Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2005 19:56:01Z, notAfter = 4/03/2008 19:56:01Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical): static CRL: thisUpdate = 7/23/2010 12:00:00Z, nextUpdate = 7/24/2010 06:00:00Z

ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ExpiredRSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://ocsp.example.com

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c (file does not exist)

4.17.6 PIV Test Card 14: Retired Key Management Certificate B

Status: not revoked

serialNumber: 1406 (0x57e)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Expired Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2006 19:56:01Z, notAfter = 4/03/2009 19:56:01Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical): static CRL: thisUpdate = 7/23/2010 12:00:00Z, nextUpdate = 7/24/2010 06:00:00Z

ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ExpiredRSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://ocsp.example.com

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c (file does not exist)

4.17.7 PIV Test Card 14: Retired Key Management Certificate C

Status: not revoked

serialNumber: 1407 (0x57f)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Expired Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2007 19:56:01Z, notAfter = 4/03/2010 19:56:01Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical): static CRL: thisUpdate = 7/23/2010 12:00:00Z, nextUpdate = 7/24/2010 06:00:00Z

ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ExpiredRSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://ocsp.example.com

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c (file does not exist)

4.17.8 PIV Test Card 14: Retired Key Management Certificate D

Status: not revoked

serialNumber: 1408 (0x580)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2008 19:56:01Z, notAfter = 4/03/2011 19:56:01Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.17.9 PIV Test Card 14: Retired Key Management Certificate E

Status: not revoked

serialNumber: 1409 (0x581)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2009 19:56:01Z, notAfter = 4/03/2012 19:56:01Z

subject: cn=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder14@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

4.18 PIV Test Card 15

4.18.1 PIV Test Card 15: PIV Authentication Certificate

Status: revoked, reason code: key compromise

serialNumber: 1501 (0x5dd)

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.13 (id-fpki-common-authentication)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D65018591C422CD9E51C6DA1625B88241A49E5A486501843E7
(Agency Code = 3201, System Code = 2722, Credential Number = 693276, CS=1, ICI=4, PI=7241649364, OC=1, OI=3201, POA=1)
UPN: 32017241649364@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.18.2 PIV Test Card 15: Card Authentication Certificate

Status: revoked, reason code: key compromise

serialNumber: 1502 (0x5de)

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: serialNumber=D65018591C422CD9E51C6DA1625B88241A49E5A486501843E7, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.6.8 (id-PIV-cardAuth)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.17 (id-fpki-common-cardAuth)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

id-piv-interim (not critical): FALSE

subjectAltName (not critical):

FASC-N: D65018591C422CD9E51C6DA1625B88241A49E5A486501843E7 (Agency Code = 3201, System Code = 2722, Credential Number = 693276, CS=1, ICI=4, PI=7241649364, OC=1, OI=3201, POA=1)

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.18.3 PIV Test Card 15: Digital Signature Certificate

Status: revoked, reason code: key compromise

serialNumber: 1503 (0x5df)

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): digitalSignature, nonRepudiation

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.18.4 PIV Test Card 15: Key Management Certificate

Status: revoked, reason code: key compromise

serialNumber: 1504 (0x5e0)

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): keyAgreement

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.18.5 PIV Test Card 15: Retired Key Management Certificate A

Status: revocation information not available

serialNumber: 1505 (0x5e1)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test RSA 1024-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 11/17/2006 17:23:14Z, notAfter = 11/17/2008 17:23:14Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SHA-1 hash of signer's public key

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical):

ldap://ldap.example.com/cn=Test%20RSA%201024-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://crl.example.com/PIVTest/RSA1024CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://ocsp.example.com

id-ad-caIssuers: ldap://ldap.example.com/cn=Test%20RSA%201024-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://p7c.example.com/PIVTest/CACertsIssuedToRSA1024CA.p7c

4.18.6 PIV Test Card 15: Retired Key Management Certificate B

Status: not revoked

serialNumber: 1506 (0x5e2)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Expired Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2007 19:56:01Z, notAfter = 4/03/2009 19:56:01Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical): static CRL: thisUpdate = 7/23/2010 12:00:00Z, nextUpdate = 7/24/2010 06:00:00Z

ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ExpiredRSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://ocsp.example.com

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c (file does not exist)

4.18.7 PIV Test Card 15: Retired Key Management Certificate C

Status: not revoked

serialNumber: 1507 (0x5e3)

signature: sha1WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Expired Test RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 4/03/2008 19:56:01Z, notAfter = 4/03/2010 19:56:01Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): keyEncipherment

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from RSA 2048 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical): static CRL: thisUpdate = 7/23/2010 12:00:00Z, nextUpdate = 7/24/2010 06:00:00Z

ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ExpiredRSA2048CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://ocsp.example.com

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Expired%20Test%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c (file does not exist)

4.18.8 PIV Test Card 15: Retired Key Management Certificate D

Status: not revoked

serialNumber: 1508 (0x5e4)

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 9/25/2008 23:18:12Z, notAfter = 9/25/2010 23:18:12Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): keyAgreement

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.18.9 PIV Test Card 15: Retired Key Management Certificate E

Status: revoked, reason code: superseded

serialNumber: 1509 (0x5e5)

signature: ecdsa-with-SHA256

issuer: cn=Test ECC P-256 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 3/12/2009 02:04:01Z, notAfter = 3/12/2011 02:04:01Z

subject: cn=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: id-ecPublicKey, P-256

Extensions:

keyUsage (critical): keyAgreement

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.3.7 (id-fpki-common-hardware)

authorityKeyIdentifier (not critical): SKI from ECC P-256 Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

rfc822Name: test.cardholder15@mail.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-256CA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

4.19 PIV-I Test Card 16

4.19.1 PIV-I Test Card 16: PIV-I Authentication Certificate

Status: not revoked

serialNumber: 1601 (0x641)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test PIV-I RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: cn=Test Cardholder XVI, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (not critical):

1.3.6.1.5.5.7.3.2 (id-kp-clientAuth)
1.3.6.1.4.1.311.20.2.2 (Microsoft Smartcardlogin)
2.5.29.37.0 (anyExtendedKeyUsage)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.48.71

authorityKeyIdentifier (not critical): SKI from RSA 2048 PIV-I Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

uniformResourceIdentifier: urn:uuid:048051b4-2288-41fd-b895-5fe9945e1c63
UPN: pivitestcardholder@upn.example.com

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048PIVICA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers:
http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048PIVICA.p7c

4.19.2 PIV-I Test Card 16: Card Authentication Certificate

Status: not revoked

serialNumber: 1602 (0x642)

signature: sha256WithRSAEncryption (PKCS #1 v1.5)

issuer: cn=Test PIV-I RSA 2048-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

validity: notBefore = 10/1/2010 08:30:00Z, notAfter = 10/1/2030 08:30:00Z

subject: serialNumber=048051b4-2288-41fd-b895-5fe9945e1c63, ou=Test Agency, ou=Test Department, o=Test Government, c=US

subjectPublicKeyInfo: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

keyUsage (critical): digitalSignature

extKeyUsage (critical): 2.16.840.1.101.3.6.8 (id-PIV-cardAuth)

certificatePolicies (not critical): 2.16.840.1.101.3.2.1.48.72

authorityKeyIdentifier (not critical): SKI from RSA 2048 PIV-I Issuing CA Certificate

subjectKeyIdentifier (not critical): SHA-1 hash of subject public key

subjectAltName (not critical):

uniformResourceIdentifier: urn:uuid:048051b4-2288-41fd-b895-5fe9945e1c63

cRLDistributionPoints (not critical):

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA2048PIVICA.crl

authorityInfoAccess (not critical):

id-ad-ocsp: http://seclab7.ncsl.nist.gov

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?cACertificate;binary,crossCertificatePair;binary

id-ad-caIssuers: http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048PIVICA.p7c

5 Acronyms

AID	Application Identifier
CA	Certification Authority
CHUID	Card Holder Unique Identifier
CRL	Certificate Revocation List
EAP	Extensible Authentication Protocol
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
FASC-N	Federal Agency Smart Credential Number
FIPS	Federal Information Processing Standard
GUID	Global Unique Identification Number
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
IPv6	Internet Protocol version 6
LAN	Local Area Network
LDAP	Lightweight Directory Access Protocol
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standards
PKINIT	Public Key based Initial Authentication in Kerberos
PPP	Point-to-Point Protocol
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman cryptographic algorithm
RSASSA-PSS	RSA Signature Scheme with Appendix - Probabilistic Signature Scheme
SHA	Secure Hash Algorithm
SP	Special Publication
TLS	Transport Layer Security
UPN	User Principal Name
URI	Uniform Resource Identifier

URN	Uniform Resource Name
UUID	Universally Unique Identifier

6 References

[FIPS201] Federal Information Processing Standard 201-1, Change Notice 1, Personal Identity Verification (PIV) Federal Employees and Contractors, March 2006.

[NISTIR7870] NIST Interagency Report 7870, *NIST Test Personal Identity Verification (PIV) Cards*, July 2012.

[SP800-73] NIST Special Publication 800-73-3, *Interfaces for Personal Identity Verification*, February 2010.

[SP800-78] NIST Special Publication 800-78-3, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, December 2010.

[RFC4122] IETF RFC 4122, "A Universally Unique Identifier (UUID) URN Namespace," July 2005.