# Technical Specifications for Personal Identity Verification (PIV) Test Cards

***Version 1.0***
***July 16, 2012***

# Table of Contents

# 1 Introduction

In order to facilitate the development of applications and middleware that support the Personal Identity Verification (PIV) Card, NIST has developed a set of test PIV Cards. This set of test cards includes not only examples that are similar to cards issued today, but also examples of cards with features that are expected to appear in cards that will be issued in the future. For example, while the certificates and data objects on most, if not all, cards issued today are signed using RSA PKCS #1 v1.5, the set of test cards include examples of certificates and data objects that are signed using each of the algorithms and key sizes listed in Table 3-3 of SP 800-78-3, including RSASSA-PSS and ECDSA. Similarly, the infrastructure supporting the test cards provides examples of CRLs and OCSP responses that are signed using each of these signature algorithms. The set of test cards also includes certificates with ECC subject public keys in addition to RSA subject public keys, as is permitted by Table 3-1 of SP 800-78-3. The set of test cards, collectively, also include all of the mandatory and optional data objects listed in Section 3 of SP 800-73-3 Part 1, except for Cardholder Iris Images. Several of the cards include a Key History object along with retired key management keys.

This document serves as a companion to NISTIR 7870, *NIST Test Personal Identity Verification (PIV) Cards* [NISTIR7870]. While NISTIR 7870 provides high-level descriptions of each of the test PIV Cards and a summary of the public key infrastructure (PKI) that supports the test PIV Cards, this document provides detailed specifications for each test card and for each certificate issued by the test PKI.

## 2 Test Card PIN Values

The table below lists all of the values for the PINs that may be used to unlock the PIV Card Applications on the test cards. In each row, the PIN value that is in **bold** is the one that the Discovery object indicates is the primary PIN used to unlock the PIV Card Application. Note that some applications do not make use of the Discovery object and so expect the PIV Card Application PIN to be entered to unlock the card, even if the Discovery object indicates that the Global PIN is the primary PIN.

| Card | PIV Card Application PIN | Global PIN |
|---|---|---|
| Test PIV Card 1 | **123456** | |
| Test PIV Card 2 | **123456** | |
| Test PIV Card 3 | 90909090 | **111111** |
| Test PIV Card 4 | **123456** | 12345678 |
| Test PIV Card 5 | **123456** | |
| Test PIV Card 6 | **123456** | |
| Test PIV Card 7 | 90909090 | **111111** |
| Test PIV Card 8 | **123456** | 12345678 |
| Test PIV Card 9 | **123456** | |
| Test PIV Card 10 | **123456** | |
| Test PIV Card 11 | **123456** | |
| Test PIV Card 12 | **123456** | |
| Test PIV Card 13 | **123456** | |
| Test PIV Card 14 | **123456** | |
| Test PIV Card 15 | **123456** | |
| Test PIV-I Card 16 | **123456** | |

# 3 Test Card Details

The table below provides a brief summary of the contents of each cards. The following subsections provide detailed information on the contents of each card.

| # | CHUID | PIV Auth | fingerprints | Facial image | Dig sig | Key man | Card auth | Discovery object | Key history |
|---|---|---|---|---|---|---|---|---|---|
| 1 | RSA 2048 PKCS #1 | RSA 2048, GZIP | Same as CHUID | Same as CHUID | RSA 2048, GZIP | RSA 2048, GZIP | RSA 2048, GZIP | Present – no global PIN | Not present |
| 2 | RSA 2048 PSS | RSA 2048, GZIP, PSS signature | Same as CHUID | Same as CHUID | RSA 2048, GZIP, PSS signature | RSA 2048, GZIP, PSS signature | RSA 2048, GZIP, PSS signature | Present – no global PIN | Present – no retired keys |
| 3 | RSA 2048 PKCS #1 | RSA 2048 | RSA 3072 PSS | Same as fingerprint | RSA 2048 | RSA 2048 | RSA 2048 | Present – global PIN is primary | 3 retired keys (1 RSA 1024, 2 RSA 2048), 3 certificates stored on card, no URL |
| 4 | ECDSA P-256 | ECDSA P-256 | Same as CHUID | Same as CHUID | ECDSA P-256 | ECDSA P-256 | ECDSA P-256 | Present – global PIN present but not primary | 5 retired keys (3 RSA 2048, 2 ECC P-256), 3 certificates stored on card |
| 5 | ECDSA P-384 | ECDSA P-256 | Same as CHUID | Same as CHUID | ECDSA P-384 | ECDSA P-384 | ECDSA P-256 | Present – no global PIN | 5 retired keys (2 RSA 2048, 2 ECC P-256, 1 ECC P-384), no certificates stored on card |
| 6 | RSA 2048 PKCS #1 | RSA 2048 | Same as CHUID | Not present | Not present | Not present | Not present | Present – no global PIN | Not present |
| 7 | RSA 2048 PKCS #1 SHA-1 | RSA 1024, SHA-1 signature | Same as CHUID | Same as CHUID | RSA 2048, SHA-1 signature | RSA 2048, SHA-1 signature | RSA 1024, SHA-1 signature | Present – global PIN is primary | 5 retired keys (1 RSA 1024, 4 RSA 2048), 3 certificates stored on card |
| 8 | RSA 2048 PKCS #1 | RSA 2048 | Same as CHUID | Same as CHUID | RSA 2048 | RSA 2048 | RSA 2048 | Present – global PIN present but not primary | 10 retired keys (2 RSA 1024, 8 RSA 2048), 3 certificates stored on card |
| 9 | RSA 2048 PKCS #1, card expired | RSA 2048, certificate expired, GZIP | Same as CHUID | Same as CHUID | RSA 2048, certificate expired, GZIP | RSA 2048, certificate expired, GZIP | RSA 2048, certificate expired, GZIP | Present – no global PIN | Not present |
| 10 | RSA 2048 PKCS #1 | RSA 2048, certificate revoked | Same as CHUID | Same as CHUID | RSA 2048, certificate revoked | RSA 2048, certificate revoked | RSA 2048, certificate revoked | Present – no global PIN | 5 retired keys (RSA 2048), 1 certificate stored on card |
| 11 | RSA 2048 PKCS #1, invalid signature | RSA 2048, invalid signature, GZIP | Same as CHUID | Same as CHUID | RSA 2048, invalid signature, GZIP | RSA 2048, invalid signature, GZIP | RSA 2048, invalid signature, GZIP | Present – no global PIN | Not present |

| # | CHUID | PIV Auth | fingerprints | Facial image | Dig sig | Key man | Card auth | Discovery object | Key history |
|---|---|---|---|---|---|---|---|---|---|
| 12 | RSA 2048 PKCS #1 | RSA 2048, FASC-N doesn't match CHUID, GZIP | FASC-N matches PIV Auth | FASC-N matches PIV Auth | RSA 2048, GZIP | RSA 2048, GZIP | FASC-N matches PIV Auth, GZIP | Present – no global PIN | Not present |
| 13 | RSA 2048 PKCS #1 | RSA 1024, expired | Same as CHUID | Same as CHUID | RSA 2048, expired | RSA 2048, expired | RSA 1024, expired | Present – no global PIN | Not present |
| 14 | RSA 2048 PKCS #1, content signer certificate revoked | RSA 2048, GZIP | Same as CHUID | Same as CHUID | RSA 2048, GZIP | RSA 2048, GZIP | RSA 2048, GZIP | Present – no global PIN | 5 retired keys (RSA 2048), 1 certificate stored on card |
| 15 | ECDSA P-256 | ECDSA P-256, certificate revoked | Same as CHUID | Same as CHUID | ECDSA P-256, certificate revoked | ECDSA P-256, certificate revoked | ECDSA P-256, certificate revoked | Present – no global PIN | 5 retired keys (1 RSA 1024, 2 RSA 2048, 2 ECC P-256), 3 certificates stored on card |
| 16 | RSA 2048 PKCS #1, PIV-I card | RSA 2048 | Same as CHUID | Same as CHUID | Not present | Not present | Not present | Present – no global PIN | Not present |

## 3.1 Test PIV Card 1

**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: 20301231
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

**PIV Authentication Certificate:**

PIV Test Card 1: PIV Authentication Certificate, GZIP compressed

**Card Authentication Certificate:**

PIV Test Card 1: Card Authentication Certificate, GZIP compressed

**Digital Signature Certificate:**

PIV Test Card 1: Digital Signature Certificate, GZIP compressed

**Key Management Certificate:**

PIV Test Card 1: 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
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012345
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

## 3.2 Test PIV Card 2

**Card Capability Container:**

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

**CHUID:**

FASC-N: D6501858289D6DC4649C25A1685A6D81208E711C86501857EE
(Agency Code = 3201, System Code = 0295, Credential Number = 723474,
CS=1, ICI=1, PI=9614127727, OC=1, OI=3201, POA=5)
GUID: all 0x00
Expiration Date: 20301231
Asymmetric signature: RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

**PIV Authentication Certificate:**

PIV Test Card 2: PIV Authentication Certificate, GZIP compressed

**Card Authentication Certificate:**

PIV Test Card 2: Card Authentication Certificate, GZIP compressed

**Digital Signature Certificate:**

PIV Test Card 2: Digital Signature Certificate, GZIP compressed

**Key Management Certificate:**

PIV Test Card 2: Key Management Certificate, GZIP compressed

**Cardholder Fingerprints:**

Indicator that no fingerprints could be obtained for cardholder

RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

**Security Object:**

RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

**Cardholder Facial Image:**

RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

**Printed Information:**

Name: Test Cardholder Jr.
Employee Affiliation: Contractor
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012346
Issuer Identification: TSTISR320161719

**Discovery Object:**

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

**Key History Object:**

*keysWithOnCardCerts* = 0, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

**Cardholder Iris Images:** Not present

## 3.3 Test PIV Card 3

**Card Capability Container:**

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

**CHUID:**

FASC-N: D650185855E56DC8127985A1645B906E7880C08286501843FC
(Agency Code = 3201, System Code = 8575, Credential Number = 714931,
CS=1, ICI=2, PI=7163720148, OC=1, OI=3201, POA=1)
GUID: 4cd8be6f-276c-47c2-af29-aa56e5acf0c9
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 3: PIV Authentication Certificate

**Card Authentication Certificate:** PIV Test Card 3: Card Authentication Certificate

**Digital Signature Certificate:** PIV Test Card 3: Digital Signature Certificate

**Key Management Certificate:** PIV Test Card 3: Key Management Certificate

**Cardholder Fingerprints:**

dummy fingerprints, RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

**Security Object:**

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

**Cardholder Facial Image:**

RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

**Printed Information:**

Name: Test Cardholder III
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012347
Issuer Identification: TSTISR320161719

**Discovery Object:**

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x60 0x20 (global PIN is primary)

**Key History Object:**

*keysWithOnCardCerts* = 3, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

key reference 82: PIV Test Card 3: Retired Key Management Key B
Certificate Tag 5FC10D: PIV Test Card 3: Retired Key Management Certificate B

key reference 83: PIV Test Card 3: Retired Key Management Key A
Certificate Tag 5FC10E: PIV Test Card 3: Retired Key Management Certificate A

key reference 84: PIV Test Card 3: Retired Key Management Key C
Certificate Tag 5FC10F: PIV Test Card 3: Retired Key Management Certificate C

**Cardholder Iris Images:** Not present

## 3.4 Test PIV Card 4

**Card Capability Container:**

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

**CHUID:**

FASC-N: D650185B3CCE6D9C9053CDA16CDA10AA09C4378486501843EB
(Agency Code = 3201, System Code = 3733, Credential Number = 334893,
CS=1, ICI=3, PI=1152472674, 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 4: PIV Authentication Certificate

**Card Authentication Certificate:** PIV Test Card 4: Card Authentication Certificate

**Digital Signature Certificate:** PIV Test Card 4: Digital Signature Certificate

**Key Management Certificate:** PIV Test Card 4: 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 E. Cardholder IV
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012348
Issuer Identification: TSTISR320161719

**Discovery Object:**

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x60 0x10 (global PIN is not primary)

**Key History Object:**

*keysWithOnCardCerts* = 3, *keysWithOffCardCerts* = 2, *offCardCertURL*:
http://smime2.nist.gov/75C4B98DFA72A1A5D266B083657FEF23739526CA6EA3D26654D9E6B84120FA35

key reference 82: PIV Test Card 4: Retired Key Management Key D
Certificate Tag 5FC10D: PIV Test Card 4: Retired Key Management Certificate D

key reference 83: PIV Test Card 4: Retired Key Management Key E
Certificate Tag 5FC10E: PIV Test Card 4: Retired Key Management Certificate E

key reference 84: PIV Test Card 4: Retired Key Management Key C
Certificate Tag 5FC10F: PIV Test Card 4: Retired Key Management Certificate C

key reference 94: PIV Test Card 4: Retired Key Management Key A

key reference 95: PIV Test Card 4: Retired Key Management Key B

**Cardholder Iris Images:** Not present

## 3.5 Test PIV Card 5

**Card Capability Container:**

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

**CHUID:**

FASC-N: D650185A13422C2267829D916CD89080501E649C86501843E2
(Agency Code = 3201, System Code = 1922, Credential Number = 843789,
CS=2, ICI=3, PI=4110207347, OC=1, OI=3201, POA=1)
GUID: 2001:0db8:0000:0000:0000:0000:0000:cd30 (IPv6 address)
Expiration Date: 20301231
Asymmetric signature: ECDSA, signed by PIV Content Signer 4

**PIV Authentication Certificate:** PIV Test Card 5: PIV Authentication Certificate

**Card Authentication Certificate:** PIV Test Card 5: Card Authentication Certificate

**Digital Signature Certificate:** PIV Test Card 5: Digital Signature Certificate

**Key Management Certificate:** PIV Test Card 5: Key Management Certificate

**Cardholder Fingerprints:** dummy fingerprints, ECDSA, signed by PIV Content Signer 4

**Security Object:** ECDSA, signed by PIV Content Signer 4

**Cardholder Facial Image:** ECDSA, signed by PIV Content Signer 4

**Printed Information:**

Name: Test E. Cardholder V
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012349
Issuer Identification: TSTISR320161719

**Discovery Object:**

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

**Key History Object:**

*keysWithOnCardCerts* = 0, *keysWithOffCardCerts* = 5, *offCardCertURL*:
http://smime2.nist.gov/776B0ED06B920A678E9249B36B628E2A4BFADD2175D15D3D217A24C6DA12ECF3

key reference 91: PIV Test Card 5: Retired Key Management Key D

key reference 92: PIV Test Card 5: Retired Key Management Key E

key reference 93: PIV Test Card 5: Retired Key Management Key C

key reference 94: PIV Test Card 5: Retired Key Management Key A

key reference 95: PIV Test Card 5: Retired Key Management Key B

**Cardholder Iris Images:** Not present

## 3.6 Test PIV Card 6

**Card Capability Container:**

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

**CHUID:**

FASC-N: D65018582214EC29D721CDA1685899207990B49086501857E4
(Agency Code = 3201, System Code = 0889, Credential Number = 895303,
CS=1, ICI=1, PI=4340730641, OC=1, OI=3201, POA=5)
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 6: PIV Authentication Certificate

**Card Authentication Certificate:** none

**Digital Signature Certificate:** none

**Key Management Certificate:** none

**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:** Not present

**Printed Information:** Not present

~~Name: Test Cardholder VI~~
~~Employee Affiliation: Contractor~~
~~Expiration date: 20301231 (2030DEC31)~~
~~Agency Card Serial Number: 0000012350~~
~~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

## 3.7 Test PIV Card 7

**Card Capability Container:**

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

**CHUID:**

FASC-N: D650185A1C84EC10850DADA166DB958121C0B61C86501843E1
(Agency Code = 3201, System Code = 1719, Credential Number = 000265, CS=1, ICI=6, PI=7514170617, OC=1, OI=3201, POA=1)
GUID: all 0x00
Expiration Date: 20301231
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-1, signed by PIV Content Signer 6

**PIV Authentication Certificate:** PIV Test Card 7: PIV Authentication Certificate

**Card Authentication Certificate:** PIV Test Card 7: Card Authentication Certificate

**Digital Signature Certificate:** PIV Test Card 7: Digital Signature Certificate

**Key Management Certificate:** PIV Test Card 7: Key Management Certificate

**Cardholder Fingerprints:**

dummy fingerprints, RSA PKCS #1 v1.5 with SHA-1, signed by PIV Content Signer 6

**Security Object:** RSA PKCS #1 v1.5 with SHA-1, signed by PIV Content Signer 6

**Cardholder Facial Image:** RSA PKCS #1 v1.5 with SHA-1, signed by PIV Content Signer 6

**Printed Information:**

Name: Test Cardholder VII
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012351
Issuer Identification: TSTISR320161719

**Discovery Object:**

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x60 0x20 (global PIN is primary)

**Key History Object:**

*keysWithOnCardCerts* = 3, *keysWithOffCardCerts* = 2, *offCardCertURL*:
http://smime2.nist.gov/B4981D95FE4128991EC53606FC83707D6C0843C2CB4360227454E79E5F7CE4A1

key reference 82: PIV Test Card 7: Retired Key Management Key E
Certificate Tag 5FC10D: PIV Test Card 7: Retired Key Management Certificate E

key reference 83: PIV Test Card 7: Retired Key Management Key C
Certificate Tag 5FC10E: PIV Test Card 7: Retired Key Management Certificate C

key reference 84: PIV Test Card 7: Retired Key Management Key D
Certificate Tag 5FC10F: PIV Test Card 7: Retired Key Management Certificate D

key reference 94: PIV Test Card 7: Retired Key Management Key B

key reference 95: PIV Test Card 7: Retired Key Management Key A

**Cardholder Iris Images:** Not present

## 3.8 Test PIV Card 8

**Card Capability Container:**

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

**CHUID:**

FASC-N: D6501859ADA92C1E56026DA1615B9545450692B086501843ED
(Agency Code = 3201, System Code = 6654, Credential Number = 075186,
CS=1, ICI=8, PI=7525816451, 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 8: PIV Authentication Certificate

**Card Authentication Certificate:** PIV Test Card 8: Card Authentication Certificate

**Digital Signature Certificate:** PIV Test Card 8: Digital Signature Certificate

**Key Management Certificate:** PIV Test Card 8: Key Management Certificate

**Cardholder Fingerprints:** one finger view, 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 VIII
Employee Affiliation: Employee
Expiration date: 20301231 (2030DEC31)
Agency Card Serial Number: 0000012352
Issuer Identification: TSTISR320161719

**Discovery Object:**

PIV Card Application AID: '4F 0B A0 …'. PIV Usage Policy: 0x60 0x10 (global PIN is not primary)

**Key History Object:**

*keysWithOnCardCerts* = 3, *keysWithOffCardCerts* = 7, *offCardCertURL*:
http://smime2.nist.gov/9be7119413b9879ca87e77e6326abc5730161b8101793380b3a52f6f4e069d99

key reference 82: PIV Test Card 8: Retired Key Management Key H
Certificate Tag 5FC10D: PIV Test Card 8: Retired Key Management Certificate H

key reference 83: PIV Test Card 8: Retired Key Management Key I
Certificate Tag 5FC10E: PIV Test Card 8: Retired Key Management Certificate I

key reference 84: PIV Test Card 8: Retired Key Management Key J
Certificate Tag 5FC10F: PIV Test Card 8: Retired Key Management Certificate J

key reference 8F: PIV Test Card 8: Retired Key Management Key E
key reference 90: PIV Test Card 8: Retired Key Management Key C
key reference 91: PIV Test Card 8: Retired Key Management Key G
key reference 92: PIV Test Card 8: Retired Key Management Key D
key reference 93: PIV Test Card 8: Retired Key Management Key F
key reference 94: PIV Test Card 8: Retired Key Management Key B
key reference 95: PIV Test Card 8: Retired Key Management Key A

**Cardholder Iris Images:** Not present

## 3.9 Test PIV Card 9

**Card Capability Container:**

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

**CHUID:**

FASC-N: D650185AA4412D084E649DA168590826784E204886501857E7
(Agency Code = 3201, System Code = 5424, Credential Number = 119949,
CS=1, ICI=1, PI=2243747282, OC=1, OI=3201, POA=5)
GUID: all 0x00
Expiration Date: 20110301
Asymmetric signature: RSA PKCS #1 v1.5 with SHA-256, signed by PIV Content Signer 1

**PIV Authentication Certificate:**

PIV Test Card 9: PIV Authentication Certificate, GZIP compressed

**Card Authentication Certificate:**

PIV Test Card 9: Card Authentication Certificate, GZIP compressed

**Digital Signature Certificate:**

PIV Test Card 9: Digital Signature Certificate, GZIP compressed

**Key Management Certificate:**

PIV Test Card 9: 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 IX
Employee Affiliation: Contractor
Expiration date: 20110301 (2011MAR01)
Agency Card Serial Number: 0000012353
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

## 3.10 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)

### 4.1.3 RSA 3072 Issuing CA Certificate

Status: not revoked

**serialNumber**: 3

**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 3072-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

**subjectPublicKeyInfo**: rsaEncryption, 3072-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%203072-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/CACertsIssuedByRSA3072CA.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)

### 4.1.5 ECC P-384 Issuing CA Certificate

Status: not revoked

**serialNumber**: 5

**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-384 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-384

**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-384%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-384CA.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

### 4.2.2 PIV Content Signer 2

Status: not revoked

**serialNumber**: 2

**signature**: RSASSA-PSS with SHA-256

**issuer**: cn=Test RSA 3072-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 2, ou=Test Department, o=Test Government, c=US

**subjectPublicKeyInfo**: rsaEncryption, 3072-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 3072 Issuing CA Certificate

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

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA3072CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%203072-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/CACertsIssuedToRSA3072CA.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

### 4.2.4 PIV Content Signer 4

Status: not revoked

**serialNumber**: 4

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 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 4, ou=Test Department, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-384

**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-384 Issuing CA Certificate

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

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-384CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%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-384CA.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

### 4.2.7 PIV Content Signer 6

Status: not revoked

**serialNumber**: 0x7380fa9343fd3a0285ac97a6042357f3ba5e509c

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

**subject**: cn=Test PIV Content Signer 6, 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

## 4.3 OCSP Responder Certificates

### 4.3.1 RSA 2048-bit CA OCSP Responder Certificate

**serialNumber**: 100,000 + x (short lifetime certificate renewed frequently)

**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 = time of issuance, notAfter = time of issuance + 24 hours

**subject**: cn=Test RSA 2048-bit CA's OCSP Responder, ou=Test CA, o=Test Government, c=US

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

**Extensions**:

**keyUsage** (critical): digitalSignature

**extKeyUsage** (not critical): 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning)

**id-pkix-OCSP-nocheck** (not critical): NULL

**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 RSA 2048 Issuing CA Certificate

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

### 4.3.2 RSA 3072-bit CA OCSP Responder Certificate

**serialNumber**: 100,000 + x (short lifetime certificate renewed frequently)

**signature**: RSASSA-PSS with SHA-256

**issuer**: cn=Test RSA 3072-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

**validity**: notBefore = time of issuance, notAfter = time of issuance + 24 hours

**subject**: cn=Test RSA 3072-bit CA's OCSP Responder, ou=Test CA, o=Test Government, c=US

**subjectPublicKeyInfo**: rsaEncryption, 3072-bit modulus, e=65537

**Extensions**:

**keyUsage** (critical): digitalSignature

**extKeyUsage** (not critical): 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning)

**id-pkix-OCSP-nocheck** (not critical): NULL

**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 RSA 3072 Issuing CA Certificate

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

### 4.3.3 ECC P-256 CA OCSP Responder Certificate

**serialNumber**: 100,000 + x (short lifetime certificate renewed frequently)

**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 = time of issuance, notAfter = time of issuance + 24 hours

**subject**: cn=Test ECC P-256 CA's OCSP Responder, ou=Test CA, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-256

**Extensions**:

**keyUsage** (critical): digitalSignature

**extKeyUsage** (not critical): 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning)

**id-pkix-OCSP-nocheck** (not critical): NULL

**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 ECC P-256 Issuing CA Certificate

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

### 4.3.4 ECC P-384 CA OCSP Responder Certificate

**serialNumber**: 100,000 + x (short lifetime certificate renewed frequently)

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

**validity**: notBefore = time of issuance, notAfter = time of issuance + 24 hours

**subject**: cn=Test ECC P-384 CA's OCSP Responder, ou=Test CA, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-384

**Extensions**:

**keyUsage** (critical): digitalSignature

**extKeyUsage** (not critical): 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning)

**id-pkix-OCSP-nocheck** (not critical): NULL

**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 ECC P-384 Issuing CA Certificate

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

### 4.3.5 RSA 2048-bit PIV-I CA OCSP Responder Certificate

**serialNumber**: 100,000 + x (short lifetime certificate renewed frequently)

**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 = time of issuance, notAfter = time of issuance + 24 hours

**subject**: cn=Test PIV-I RSA 2048-bit CA's OCSP Responder, ou=Test CA, o=Test Government, c=US

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

**Extensions**:

**keyUsage** (critical): digitalSignature

**extKeyUsage** (not critical): 1.3.6.1.5.5.7.3.9 (id-kp-OCSPSigning)

**id-pkix-OCSP-nocheck** (not critical): NULL

**certificatePolicies** (not critical):

2.16.840.1.101.3.2.1.48.71
2.16.840.1.101.3.2.1.48.72
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

## 4.4 PIV Test Card 1

### 4.4.1 PIV Test Card 1: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 101 (0x65)

**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, 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

### 4.4.2 PIV Test Card 1: Card Authentication Certificate

Status: not revoked

**serialNumber**: 102 (0x66)

**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=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

### 4.4.3 PIV Test Card 1: Digital Signature Certificate

Status: not revoked

**serialNumber**: 103 (0x67)

**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, 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

### 4.4.4 PIV Test Card 1: Key Management Certificate

Status: not revoked

**serialNumber**: 104 (0x68)

**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, 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

## 4.5 PIV Test Card 2

### 4.5.1 PIV Test Card 2: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 201 (0xc9)

**signature**: RSASSA-PSS with SHA-256

**issuer**: cn=Test RSA 3072-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 Jr. (affiliate), ou=Test Agency, ou=Test Department, o=Test Government, c=US

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

**Extensions**:

**keyUsage** (critical): digitalSignature

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

**authorityKeyIdentifier** (not critical): SKI from RSA 3072 Issuing CA Certificate

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

**id-piv-interim** (not critical): FALSE

**subjectAltName** (not critical):

FASC-N: D6501858289D6DC4649C25A1685A6D81208E711C86501857EE
(Agency Code = 3201, System Code = 0295, Credential Number = 723474, CS=1, ICI=1, PI=9614127727, OC=1, OI=3201, POA=5)

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA3072CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%203072-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/CACertsIssuedToRSA3072CA.p7c

### 4.5.2 PIV Test Card 2: Card Authentication Certificate

Status: not revoked

**serialNumber**: 202 (0xca)

**signature**: RSASSA-PSS with SHA-256

**issuer**: cn=Test RSA 3072-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**: (null)

**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 3072 Issuing CA Certificate

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

**id-piv-interim** (not critical): FALSE

**subjectAltName** (critical):

FASC-N: D6501858289D6DC4649C25A1685A6D81208E711C86501857EE
(Agency Code = 3201, System Code = 0295, Credential Number = 723474, CS=1, ICI=1, PI=9614127727, OC=1, OI=3201, POA=5)

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA3072CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%203072-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/CACertsIssuedToRSA3072CA.p7c

### 4.5.3 PIV Test Card 2: Digital Signature Certificate

Status: not revoked

**serialNumber**: 203 (0xcb)

**signature**: RSASSA-PSS with SHA-256

**issuer**: cn=Test RSA 3072-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 Jr. (affiliate), 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 3072 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: test.cardholder2@mail.example.com

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA3072CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%203072-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/CACertsIssuedToRSA3072CA.p7c

### 4.5.4 PIV Test Card 2: Key Management Certificate

Status: not revoked

**serialNumber**: 204 (0xcc)

**signature**: RSASSA-PSS with SHA-256

**issuer**: cn=Test RSA 3072-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 Jr. (affiliate), 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 3072 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: test.cardholder2@mail.example.com

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/RSA3072CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20RSA%203072-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/CACertsIssuedToRSA3072CA.p7c

## 4.6 PIV Test Card 3

### 4.6.1 PIV Test Card 3: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 301 (0x12d)

**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=D650185855E56DC8127985A1645B906E7880C08286501843FC, 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)
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: D650185855E56DC8127985A1645B906E7880C08286501843FC (Agency Code = 3201, System Code = 8575, Credential Number = 714931, CS=1, ICI=2, PI=7163720148, OC=1, OI=3201, POA=1)
uniformResourceIdentifier: urn:uuid:4cd8be6f-276c-47c2-af29-aa56e5acf0c9

**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

### 4.6.2 PIV Test Card 3: Card Authentication Certificate

Status: not revoked

**serialNumber**: 302 (0x12e)

**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=D650185855E56DC8127985A1645B906E7880C08286501843FC, 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: D650185855E56DC8127985A1645B906E7880C08286501843FC (Agency Code = 3201, System Code = 8575, Credential Number = 714931, CS=1, ICI=2, PI=7163720148, OC=1, OI=3201, POA=1)

uniformResourceIdentifier: urn:uuid:4cd8be6f-276c-47c2-af29-aa56e5acf0c9

**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

### 4.6.3 PIV Test Card 3: Digital Signature Certificate

Status: not revoked

**serialNumber**: 303 (0x12f)

**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 III, 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.cardholder3@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

### 4.6.4 PIV Test Card 3: Key Management Certificate

Status: not revoked

**serialNumber**: 304 (0x130)

**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 III, 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.cardholder3@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

### 4.6.5 PIV Test Card 3: Retired Key Management Certificate A

Status: revocation information not available

**serialNumber**: 305 (0x131)

**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 Cardholder III, 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.cardholder3@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

### 4.6.6 PIV Test Card 3: Retired Key Management Certificate B

Status: not revoked

**serialNumber**: 306 (0x132)

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

**subject**: cn=Test Cardholder III, 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.cardholder3@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

### 4.6.7 PIV Test Card 3: Retired Key Management Certificate C

Status: revoked

**serialNumber**: 307 (0x133)

**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 = 7/26/2008 20:12:48Z, notAfter = 7/26/2028 20:12:48Z

**subject**: cn=Test Cardholder III, 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.cardholder3@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

## 4.7 PIV Test Card 4

### 4.7.1 PIV Test Card 4: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 401 (0x191)

**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 IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-256

**Extensions**:

**keyUsage** (critical): digitalSignature

**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: D650185B3CCE6D9C9053CDA16CDA10AA09C4378486501843EB
(Agency Code = 3201, System Code = 3733, Credential Number = 334893, CS=1, ICI=3, PI=1152472674, OC=1, OI=3201, POA=1)
UPN: 32011152472674@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

### 4.7.2 PIV Test Card 4: Card Authentication Certificate

Status: not revoked

**serialNumber**: 402 (0x192)

**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=D650185B3CCE6D9C9053CDA16CDA10AA09C4378486501843EB, 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: D650185B3CCE6D9C9053CDA16CDA10AA09C4378486501843EB (Agency Code = 3201, System Code = 3733, Credential Number = 334893, CS=1, ICI=3, PI=1152472674, 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

### 4.7.3 PIV Test Card 4: Digital Signature Certificate

Status: not revoked

**serialNumber**: 403 (0x193)

**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 IV, 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.cardholder4@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

### 4.7.4 PIV Test Card 4: Key Management Certificate

Status: not revoked

**serialNumber**: 404 (0x194)

**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 IV, 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.cardholder4@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

### 4.7.5 PIV Test Card 4: Retired Key Management Certificate A

Status: not revoked

**serialNumber**: 405 (0x195)

**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 E. Cardholder IV, 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.cardholder4@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)

### 4.7.6 PIV Test Card 4: Retired Key Management Certificate B

Status: not revoked

**serialNumber**: 406 (0x196)

**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 = 5/19/2006 19:56:01Z, notAfter = 5/19/2009 19:56:01Z

**subject**: cn=Test E. Cardholder IV, 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.cardholder4@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)

### 4.7.7 PIV Test Card 4: Retired Key Management Certificate C

Status: not revoked

**serialNumber**: 407 (0x197)

**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 = 3/02/2007 11:17:23Z, notAfter = 3/02/2010 11:17:23Z

**subject**: cn=Test E. Cardholder IV, 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.cardholder4@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)

### 4.7.8 PIV Test Card 4: Retired Key Management Certificate D

Status: revoked, reason code: superseded

**serialNumber**: 408 (0x198)

**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 = 9/25/2011 23:18:12Z

**subject**: cn=Test E. Cardholder IV, 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.cardholder4@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

### 4.7.9 PIV Test Card 4: Retired Key Management Certificate E

Status: revoked, reason code: key compromise

**serialNumber**: 409 (0x199)

**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 = 3/12/2012 02:04:01Z

**subject**: cn=Test E. Cardholder IV, 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.cardholder4@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

## 4.8 PIV Test Card 5

### 4.8.1 PIV Test Card 5: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 501 (0x1f5)

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 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 V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-256

**Extensions**:

**keyUsage** (critical): digitalSignature

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

**authorityKeyIdentifier** (not critical): SKI from ECC P-384 Issuing CA Certificate

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

**id-piv-interim** (not critical): FALSE

**subjectAltName** (not critical):

FASC-N: D650185A13422C2267829D916CD89080501E649C86501843E2
(Agency Code = 3201, System Code = 1922, Credential Number = 843789, CS=2, ICI=3, PI=4110207347, OC=1, OI=3201, POA=1)

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-384CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%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-384CA.p7c

### 4.8.2 PIV Test Card 5: Card Authentication Certificate

Status: not revoked

**serialNumber**: 502 (0x1f6)

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 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=D650185A13422C2267829D916CD89080501E649C86501843E2, 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-384 Issuing CA Certificate

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

**id-piv-interim** (not critical): FALSE

**subjectAltName** (not critical):

FASC-N: D650185A13422C2267829D916CD89080501E649C86501843E2 (Agency Code = 3201, System Code = 1922, Credential Number = 843789, CS=2, ICI=3, PI=4110207347, OC=1, OI=3201, POA=1)

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-384CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%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-384CA.p7c

### 4.8.3 PIV Test Card 5: Digital Signature Certificate

Status: not revoked

**serialNumber**: 503 (0x1f7)

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 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 V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-384

**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-384 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: test.cardholder5@mail.example.com

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-384CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%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-384CA.p7c

### 4.8.4 PIV Test Card 5: Key Management Certificate

Status: not revoked

**serialNumber**: 504 (0x1f8)

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 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 V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

**subjectPublicKeyInfo**: id-ecPublicKey, P-384

**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-384 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: test.cardholder5@mail.example.com

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-384CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%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-384CA.p7c

### 4.8.5 PIV Test Card 5: Retired Key Management Certificate A

Status: not revoked

**serialNumber**: 505 (0x1f9)

**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 E. Cardholder V, 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.cardholder5@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)

### 4.8.6 PIV Test Card 5: Retired Key Management Certificate B

Status: not revoked

**serialNumber**: 506 (0x1fa)

**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 = 5/19/2006 19:56:01Z, notAfter = 5/19/2009 19:56:01Z

**subject**: cn=Test E. Cardholder V, 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.cardholder5@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)

### 4.8.7 PIV Test Card 5: Retired Key Management Certificate C

Status: not revoked

**serialNumber**: 507 (0x1fb)

**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 = 9/25/2007 23:18:12Z, notAfter = 9/25/2010 23:18:12Z

**subject**: cn=Test E. Cardholder V, 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.cardholder5@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

### 4.8.8 PIV Test Card 5: Retired Key Management Certificate D

Status: not revoked

**serialNumber**: 508 (0x1fc)

**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 = 9/25/2011 23:18:12Z

**subject**: cn=Test E. Cardholder V, 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.cardholder5@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

### 4.8.9 PIV Test Card 5: Retired Key Management Certificate E

Status: not revoked

**serialNumber**: 509 (0x1fd)

**signature**: ecdsa-with-SHA384

**issuer**: cn=Test ECC P-384 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

**validity**: notBefore = 9/25/2009 23:18:12Z, notAfter = 9/25/2012 23:18:12Z

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

**subjectPublicKeyInfo**: id-ecPublicKey, P-384

**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-384 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: test.cardholder5@mail.example.com

**cRLDistributionPoints** (not critical):

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards,ou=Test%20CA,o=Test%20Certificates%202010,c=US?certificateRevocationList;binary

http://smime2.nist.gov/PIVTest/ECCP-384CA.crl

**authorityInfoAccess** (not critical):

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

id-ad-caIssuers: ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%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-384CA.p7c

## 4.9 PIV Test Card 6

### 4.9.1 PIV Test Card 6: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 601 (0x259)

**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=D65018582214EC29D721CDA1685899207990B49086501857E4, ou=Test Agency, ou=Test Department, o=Test Government, c=US

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

**Extensions**:

**keyUsage** (critical): digitalSignature

**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): TRUE

**subjectAltName** (critical):

FASC-N: D65018582214EC29D721CDA1685899207990B49086501857E4 (Agency Code = 3201, System Code = 0889, Credential Number = 895303, CS=1, ICI=1, PI=4340730641, OC=1, OI=3201, POA=5)

**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

## 4.10 PIV Test Card 7

### 4.10.1 PIV Test Card 7: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 701 (0x2bd)

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

**subject**: cn=Test Cardholder VII, 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: D650185A1C84EC10850DADA166DB958121C0B61C86501843E1
(Agency Code = 3201, System Code = 1719, Credential Number = 000265, CS=1, ICI=6, PI=7514170617, OC=1, OI=3201, POA=1)
UPN: testcardholder7@upn.example.net

**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

### 4.10.2 PIV Test Card 7: Card Authentication Certificate

Status: not revoked

**serialNumber**: 702 (0x2be)

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

**subject**: serialNumber=D650185A1C84EC10850DADA166DB958121C0B61C86501843E1, 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: D650185A1C84EC10850DADA166DB958121C0B61C86501843E1 (Agency Code = 3201, System Code = 1719, Credential Number = 000265, CS=1, ICI=6, PI=7514170617, 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

### 4.10.3 PIV Test Card 7: Digital Signature Certificate

Status: not revoked

**serialNumber**: 703 (0x2bf)

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

**subject**: cn=Test Cardholder VII, 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.cardholder7@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

### 4.10.4 PIV Test Card 7: Key Management Certificate

Status: not revoked

**serialNumber**: 704 (0x2c0)

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

**subject**: cn=Test Cardholder VII, 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.cardholder7@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

### 4.10.5 PIV Test Card 7: Retired Key Management Certificate A

Status: not revoked

**serialNumber**: 705 (0x2c1)

**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 = 5/19/2005 19:56:01Z, notAfter = 5/19/2008 19:56:01Z

**subject**: cn=Test Cardholder VII, 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): SKI from RSA 2048 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: test.cardholder7@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)

### 4.10.6 PIV Test Card 7: Retired Key Management Certificate B

Status: not revoked

**serialNumber**: 706 (0x2c2)

**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 = 5/19/2006 19:56:01Z, notAfter = 5/19/2009 19:56:01Z

**subject**: cn=Test Cardholder VII, 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.cardholder7@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)

### 4.10.7 PIV Test Card 7: Retired Key Management Certificate C

Status: not revoked

**serialNumber**: 707 (0x2c3)

**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 = 5/19/2007 19:56:01Z, notAfter = 5/19/2010 19:56:01Z

**subject**: cn=Test Cardholder VII, 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.cardholder7@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)

### 4.10.8 PIV Test Card 7: Retired Key Management Certificate D

Status: not revoked

**serialNumber**: 708 (0x2c4)

**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 = 5/19/2008 19:56:01Z, notAfter = 5/19/2011 19:56:01Z

**subject**: cn=Test Cardholder VII, 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.cardholder7@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)

### 4.10.9 PIV Test Card 7: Retired Key Management Certificate E

Status: not revoked

**serialNumber**: 709 (0x2c5)

**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 = 5/19/2009 19:56:01Z, notAfter = 5/19/2012 19:56:01Z

**subject**: cn=Test Cardholder VII, 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.cardholder7@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)

## 4.11 PIV Test Card 8

### 4.11.1 PIV Test Card 8: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 0x0347af74f116c3e62b8516e8dd4f9e2dea460a41

**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 VIII, 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)
1.3.6.1.5.2.3.4 (id-pkinit-KPClientAuth)
1.3.6.1.5.5.7.3.13 (id-kp-eapOverPPP)
1.3.6.1.5.5.7.3.14 (id-kp-eapOverLAN)
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): TRUE

**subjectAltName** (not critical):

FASC-N: D6501859ADA92C1E56026DA1615B9545450692B086501843ED
(Agency Code = 3201, System Code = 6654, Credential Number = 075186, CS=1, ICI=8, PI=7525816451, OC=1, OI=3201, POA=1)
UPN: 32017525816451@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

### 4.11.2 PIV Test Card 8: Card Authentication Certificate

Status: not revoked

**serialNumber**: 0x11b28ebcc7904431a1ff6fed018632e1

**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=D6501859ADA92C1E56026DA1615B9545450692B086501843ED, 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): TRUE

**subjectAltName** (not critical):

FASC-N: D6501859ADA92C1E56026DA1615B9545450692B086501843ED (Agency Code = 3201, System Code = 6654, Credential Number = 075186, CS=1, ICI=8, PI=7525816451, 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

### 4.11.3 PIV Test Card 8: Digital Signature Certificate

Status: not revoked

**serialNumber**: 0x3568fcf64a1160a4

**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 VIII, 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.cardholder8@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

### 4.11.4 PIV Test Card 8: Key Management Certificate

Status: not revoked

**serialNumber**: 0x5822b65e8360b23d893d45783721dc

**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 VIII, 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.cardholder8@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

### 4.11.5 PIV Test Card 8: Retired Key Management Certificate A

Status: not revoked

**serialNumber**: 805 (0x325)

**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 = 5/19/2005 19:56:01Z, notAfter = 5/19/2008 19:56:01Z

**subject**: cn=Example Cardholder, 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): SKI from RSA 2048 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: example.cardholder@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)

### 4.11.6 PIV Test Card 8: Retired Key Management Certificate B

Status: not revoked

**serialNumber**: 806 (0x326)

**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 = 6/19/2005 19:56:01Z, notAfter = 6/19/2008 19:56:01Z

**subject**: cn=Example Cardholder, 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): SKI from RSA 2048 Issuing CA Certificate

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

**subjectAltName** (not critical):

rfc822Name: example.cardholder@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)

### 4.11.7 PIV Test Card 8: Retired Key Management Certificate C

Status: not revoked

**serialNumber**: 807 (0x327)

**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 = 7/19/2005 19:56:01Z, notAfter = 7/19/2008 19:56:01Z

**subject**: cn=Example 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: example.cardholder@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)

### 4.11.8 PIV Test Card 8: Retired Key Management Certificate D

Status: not revoked

**serialNumber**: 808 (0x328)

**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 = 8/19/2005 19:56:01Z, notAfter = 8/19/2008 19:56:01Z

**subject**: cn=Example 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: example.cardholder@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)

### 4.11.9 PIV Test Card 8: Retired Key Management Certificate E

Status: not revoked

**serialNumber**: 809 (0x329)

**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 = 9/19/2005 19:56:01Z, notAfter = 9/19/2008 19:56:01Z

**subject**: cn=Example 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: example.cardholder@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)

### 4.11.10 PIV Test Card 8: Retired Key Management Certificate F

Status: not revoked

**serialNumber**: 810 (0x32a)

**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 = 10/19/2005 19:56:01Z, notAfter = 10/19/2008 19:56:01Z

**subject**: cn=Example 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: example.cardholder@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)

### 4.11.11 PIV Test Card 8: Retired Key Management Certificate G

Status: not revoked

**serialNumber**: 811 (0x32b)

**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 = 11/19/2005 19:56:01Z, notAfter = 11/19/2008 19:56:01Z

**subject**: cn=Example 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: example.cardholder@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)

### 4.11.12 PIV Test Card 8: Retired Key Management Certificate H

Status: not revoked

**serialNumber**: 812 (0x32c)

**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 = 12/19/2005 19:56:01Z, notAfter = 12/19/2008 19:56:01Z

**subject**: cn=Example 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: example.cardholder@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)

### 4.11.13 PIV Test Card 8: Retired Key Management Certificate I

Status: not revoked

**serialNumber**: 813 (0x32d)

**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 = 7/26/2008 20:12:48Z, notAfter = 7/26/2011 20:12:48Z

**subject**: cn=Test Cardholder VIII, 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.cardholder8@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

### 4.11.14 PIV Test Card 8: Retired Key Management Certificate J

Status: not revoked

**serialNumber**: 814 (0x32e)

**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 = 7/26/2009 20:12:48Z, notAfter = 7/26/2012 20:12:48Z

**subject**: cn=Test Cardholder VIII, 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.cardholder8@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

## 4.12 PIV Test Card 9

### 4.12.1 PIV Test Card 9: PIV Authentication Certificate

Status: not revoked

**serialNumber**: 901 (0x385)

**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 = 3/1/2011 08:30:00Z

**subject**: cn=Test Cardholder IX (affiliate), 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): TRUE

**subjectAltName** (not critical):

FASC-N: D650185AA4412D084E649DA168590826784E204886501857E7
(Agency Code = 3201, System Code = 5424, Credential Number = 119949, CS=1, ICI=1, PI=2243747282, OC=1, OI=3201, POA=5)
UPN: 32012243747282@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

### 4.12.2 PIV Test Card 9: Card Authentication Certificate

Status: not revoked

**serialNumber**: 902 (0x386)

**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 = 3/1/2011 08:30:00Z

**subject**: serialNumber=D650185AA4412D084E649DA168590826784E204886501857E7, 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): TRUE

**subjectAltName** (not critical):

FASC-N: D650185AA4412D084E649DA168590826784E204886501857E7 (Agency Code = 3201, System Code = 5424, Credential Number = 119949, CS=1, ICI=1, PI=2243747282, OC=1, OI=3201, POA=5)

**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

### 4.12.3 PIV Test Card 9: Digital Signature Certificate

Status: not revoked

**serialNumber**: 903 (0x387)

**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 = 3/1/2011 08:30:00Z

**subject**: cn=Test Cardholder IX (affiliate), 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.cardholder9@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

### 4.12.4 PIV Test Card 9: Key Management Certificate

Status: not revoked

**serialNumber**: 904 (0x388)

**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 = 3/1/2011 08:30:00Z

**subject**: cn=Test Cardholder IX (affiliate), 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.cardholder9@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

## 4.13 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

### 4.13.2 PIV Test Card 10: Card Authentication Certificate

Status: revoked, reason code: key compromise

**serialNumber**: 1002 (0x3ea)

**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=D650185A0D412D5AB49915A16CDA75257286D6B086501843E2, 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: D650185A0D412D5AB49915A16CDA75257286D6B086501843E2 (Agency Code = 3201, System Code = 1624, Credential Number = 556438, CS=1, ICI=3, PI=9545326551, 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

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

Status: revoked, reason code: key compromise

**serialNumber**: 1003 (0x3eb)

**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, 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.cardholder10@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

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

Status: revoked, reason code: key compromise

**serialNumber**: 1004 (0x3ec)

**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): 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.cardholder10@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

### 4.13.5 PIV Test Card 10: Retired Key Management Certificate A

Status: not revoked

**serialNumber**: 1005 (0x3ed)

**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 X, 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.cardholder10@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)

### 4.13.6 PIV Test Card 10: Retired Key Management Certificate B

Status: not revoked

**serialNumber**: 1006 (0x3ee)

**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 X, 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.cardholder10@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)

### 4.13.7 PIV Test Card 10: Retired Key Management Certificate C

Status: not revoked

**serialNumber**: 1007 (0x3ef)

**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 X, 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.cardholder10@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)

### 4.13.8 PIV Test Card 10: Retired Key Management Certificate D

Status: revoked, reason code: key compromise

**serialNumber**: 1008 (0x3f0)

**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 X, 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.cardholder10@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

### 4.13.9 PIV Test Card 10: Retired Key Management Certificate E

Status: revoked, reason code: key compromise

**serialNumber**: 1009 (0x3f1)

**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 X, 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.cardholder10@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 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.