NISTIR 8347

NIST Test Personal Identity Verification (PIV) Cards Version 2

David A. Cooper

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8347

National Institute of
Standards and Technology
U.S. Department of Commerce

NISTIR 8347

NIST Test Personal Identity Verification (PIV) Cards Version 2

David A. Cooper
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8347

April 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Interagency or Internal Report 8347
191 pages (April 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8347

Comments on this publication may be submitted to:

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: piv-test-cards-comments@nist.gov

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems.

Abstract

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 and a supporting public key infrastructure (PKI). 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. This document provides an overview of the test cards, the infrastructure that has been developed to support their use, and detailed specifications for each test card and for each certificate issued by the test PKI.

Keywords

Homeland Security Presidential Directive-12; HSPD-12; Personal Identity Verification; PIV; PKI; public key infrastructure.

Table of Contents

List of Appendices

List of Figures

List of Tables

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 and a supporting public key infrastructure. 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 includes examples of certificates and data objects that are signed using each of the algorithms and key sizes listed in Table 3-3 of [SP800-78], including RSASSA-PSS and ECDSA. Similarly, the infrastructure supporting the test cards provides examples of certificate revocation lists (CRLs) and Online Certificate Status Protocol (OCSP) responses that are signed using each of these signature algorithms. The set of test cards also includes certificates with elliptic curve cryptography (ECC) subject public keys in addition to RSA subject public keys, as is permitted by Table 3-1 of [SP800-78]. Collectively, the set of test cards also includes all of the mandatory and optional data objects listed in Section 3 of [SP800-73] Part 1, except for Cardholder Iris Images. Several of the cards include a Key History object along with retired key management keys.

Version 2 of the test cards, which is described in this document, is similar to the initial version of the test cards, which is described in [NISTIR7870]. Changes were made, however, so that all of the version 2 test cards comply with FIPS 201-2, SP 800-73-4, and SP 800-78-4. Since any PIV Cards that are valid at the time this document is published should have been issued in accordance with these versions of the documents, there should be no need to check whether applications work with cards issued under the older versions of the standard. For example, none of the test cards include signatures generated using SHA-1, and every test card includes a UUID in the GUID data element of the CHUID. Some of the version 2 test cards also include optional features from SP 800-73-4 that did not appear in SP 800-73-3, such as secure messaging and the virtual contact interface.

2 Test Public Key Infrastructure

The cardholders' certificates and the content signers' certificates of the test PIV Cards are issued from a simple, two-level hierarchical public key infrastructure (PKI), as depicted in Figure 1. The root certification authority (CA) has issued certificates to several intermediate CAs, which in turn have issued the end-entity certificates. In order to be able to validate the certificates of the test cards, it will be necessary to install the root CA from the PKI as a trust anchor in the software that will be validating the certificates. A self-signed CA certificate for the root CA, which may be used to establish the root CA as a trust anchor, is available at https://csrc.nist.gov/projects/piv/nist-piv-test-cards.

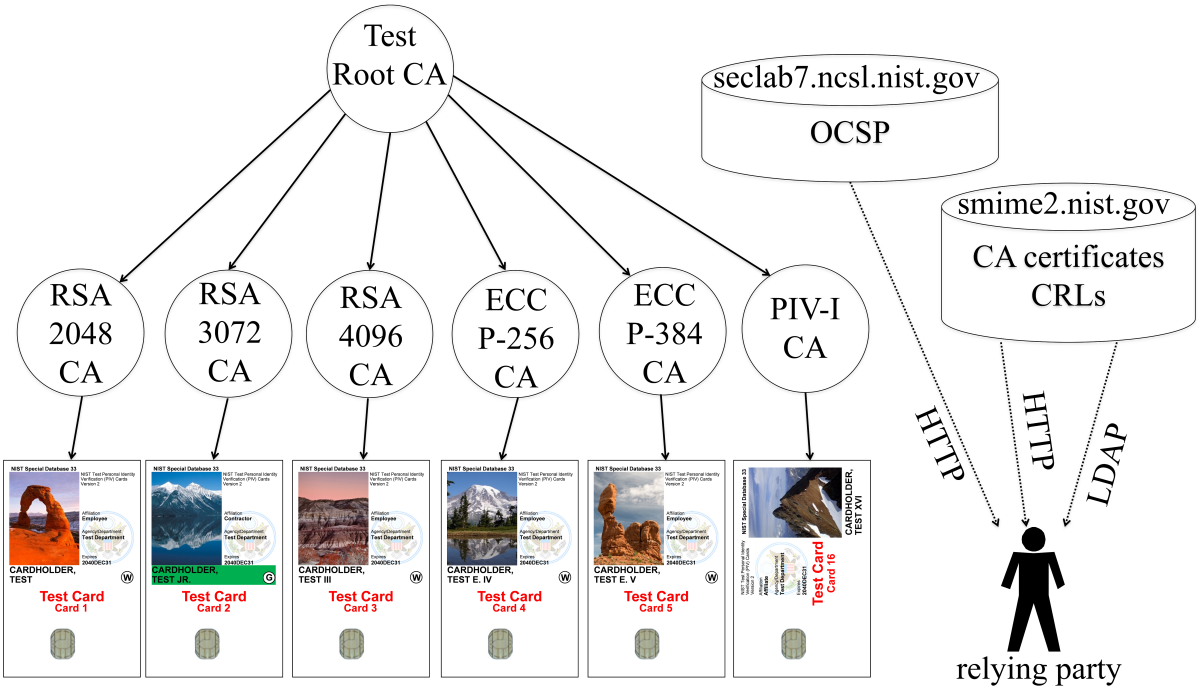

Figure 1 - PKI for Test PIV Cards

The test PKI includes examples of certificates using each of the public key sizes and signature algorithms permitted by [SP800-78]. The test PKI also includes some certificates that contain 4096-bit RSA public keys and that are signed using RSA PKCS #1 v1.5 with SHA-384 or SHA-512. While these are not permitted by [SP800-78], they are permitted by [COMMON] and may be permitted by a future update to [SP800-78].

The test PKI includes a server that provides access to CA certificates and CRLs via both Lightweight Directory Access Protocol (LDAP) and Hypertext Transfer Protocol (HTTP). Each certificate issued by the PKI, except for the self-signed certificate issued by the root CA, includes a cRLDistributionPoints extension with an HTTP URI that points to the relevant CRL for that certificate, and many of the certificates also include an LDAP URI. Each of these certificates also includes an authorityInfoAccess extension with an HTTP URI that points to the location where the CA certificates issued to the issuer of the certificate may be found, with many

of the certificates also including an LDAP URI. The self-signed certificate issued by the root CA includes a subjectInfoAccess extension with both HTTP and LDAP URIs that point to the location where the CA certificates issued by the root may be found. While some certificate validation software can use the URIs in the certificates to automatically retrieve the intermediate CA certificates needed to validate the end-entity certificates in the test PKI, some certificate validation software will only be able to validate the end-entity certificates if the intermediate CA certificates are installed manually. In order to support such software, the intermediate CA certificates have been made available at https://csrc.nist.gov/projects/piv/nist-piv-test-cards.

The test PKI also includes an OCSP responder that provides revocation status information for each of the unexpired end-entity certificates in the PKI. Each of the end-entity certificates includes an HTTP URI in its authorityInfoAccess extension that points to the OCSP responder. The root CA issues CRLs once every 15 days, with the CRLs specifying a nextUpdate time that is 31 days after the CRL was issued. The CAs that issue the end-entity certificates issue CRLs once every 12 hours, with the CRLs specifying a nextUpdate time that is 48 hours after the CRL was issued. The OCSP responder only provides pre-signed responses, which are also produced once every 12 hours. The nextUpdate time indicated for each certificate in the OCSP responses is 48 hours after the OCSP response was produced.

The server that provides access to the CA certificates and CRLs also provides access to the retired key management certificates for test cards that include a Key History object with an *offCardCertURL*. These certificates are available via HTTP, as specified in the *offCardCertURL*.

The URIs in many of the expired certificates refer to locations that do not exist. This was done to emphasize that there is no need to validate retired certificates for key management and that repositories supporting CAs that are no longer operational may not be available.

3 Biometric Data

The minutiae records for Cardholder Fingerprints data objects were created from synthetic fingerprints, which were generated using the Synthetic Fingerprint Generator (SFinGe) from the Biometric System Laboratory at the University of Bologna.[1] The fingerprint on the left in Figure 2 was used as the left index finger, and the fingerprint on the right was used as the right index finger. The image for the right index finger was used in minutiae records for every card except Test PIV Card 2, and the image for the left index finger was used in minutiae records for every card except Test PIV Cards 2 and 7. Test PIV Card 2 represents a card holder from whom no fingerprint data could be collected, and Test PIV Card 7 represents a card holder from whom fingerprint data could only be collected from one finger.

Figure 2 - Synthetic Fingerprints for Test Cards

Test PIV Card 8 is configured to support on-card biometric comparison (OCC). As [FIPS201] and [SP800-76] recommend that different fingers be used for on-card and off-card comparison, the Biometric Information Templates (BIT) Group Template indicates that the left and right middle fingers may be used for on-card biometric comparison. In generating the OCC data, the fingerprint on the left in Figure 2 was used as the left middle finger, and the fingerprint on the right was used as the right middle finger. The following are examples of application protocol data units (APDU) that may be used to successfully perform the VERIFY command using OCC data on Test PIV Card 8:

00:20:00:96:7B:6E:29:BA:81:2F:79:4A:38:AB:3F:40:6B:81:43:75:58:45:73:64:49:B4:45:4B:B0:25:52:AC:53:52:72:31:55:AE:3C:57:B0:8E:59:B5:9A:62:76:5C:65:53:2B:68:B0:4E:69:B4:3E:79:72:AE:80:B6:1D:81:AF:86:87:B6:2A:90:B3:40:93:B5:73:94:B6:24:95:B1:8F:9C:96:6F:9C:95:A5:AA:97:45:AF:56:68:AF:98:29:B8:96:84:BC:57:21:BD:57:3F:C0:58:92:C2:78:4A:C9:99:34:D0:9A:8D:D3:99:5C:D6:5A:49:E3:5B:75:ED:9A

00:20:00:97:4E:76:38:7A:5D:45:5C:31:4C:A5:8B:63:B6:50:69:5F:44:6A:66:75:70:B4:6A:71:72:4C:72:A7:81:8A:B4:97:8E:78:A6:9F:99:67:A1:8A:34:A3:89:45:A9:47:78:AE:BF:6E:AF:85:88:B3:9F:61:B8:84:9D:BA:5C:4B:C1:85:9E:D6:9E:4E:D7:84:63:DC:42:83:E4:7F:6F:EB:81

The images that appear on the faces of the test cards and in the Cardholder Facial Image data objects are all images from national parks extracted from public domain photographs available on the National Park Service website.[2]

[1] See http://biolab.csr.unibo.it/research.asp?organize=Activities&select=&selObj=12&pathSubj=111||12&.
[2] See https://www.nps.gov/index.htm.

4 Overview of Test PIV Cards

This section provides a brief overview of each of the test cards.

Test PIV Card 1:

Test PIV Card 1 is intended to represent the type of card that may be issued by a production system today. Test PIV Card 1 contains many of the optional data objects specified in [SP800-73] but none of the data objects that were newly specified in SP 800-73-4. All of the certificates on Test PIV Card 1 contain 2048-bit RSA public keys, and all of the certificates and data objects are signed using RSA PKCS #1 v1.5 with SHA-256. The PIV Authentication certificate on Test PIV Card 1 includes a User Principal Name (UPN) in the subjectAltName extension and has an extended key usage extension that asserts the client authentication, smart card logon, and PKINIT [RFC4556] object identifiers (OIDs). Test PIV Card 1 includes a Key History object indicating that one retired key management key and its corresponding certificate are stored on the card.

Test PIV Card 2:

Test PIV Card 2 is similar to Test PIV Card 1, except that certificates and data objects are signed using RSASSA-PSS rather than RSA PKCS #1 v1.5, and CAs, OCSP responders, and content signers use 3072-bit RSA keys rather than 2048-bit RSA keys. Other differences are that the cardholder is a contractor rather than an employee, and the PIV Authentication certificate does not include a UPN in the subjectAltName extension. The Card Authentication certificate on Test PIV Card 2 is the only certificate in the test set that has an empty subject name. The fingerprint data object does not contain any finger views since none of the cardholder's fingerprints could be imaged. Test PIV Card 2 supports secure messaging using cipher suite 7 and also implements the virtual contact interface (VCI).

Test PIV Card 3:

Like Test PIV Card 1, the certificates on Test PIV Card 3 contain 2048-bit RSA keys and are signed using RSA PKCS #1 v1.5 with SHA-256. However, Test PIV Card 3 differs from Test PIV Card 1 and Test PIV Card 2 in a number of ways. The PIV Authentication certificate on Test PIV Card 3 includes an extended key usage extension that asserts the client authentication and smart card logon OIDs but not PKINIT. The subject name in the PIV Authentication certificate contains the card's FASC-N rather than the cardholder's name. The PIV Authentication certificate also does not include a UPN in the subjectAltName extension. Test PIV Card 3 includes a Discovery object that indicates that the Global PIN may be used to unlock the PIV Card Application and that the Global PIN is the primary PIN used to unlock the PIV Card Application. Test PIV Card 3 is the only card in the set of test cards for which the biometric data objects are signed using a different key than the CHUID and the Security Object. Finally, Test PIV Card 3 includes a Key History object that indicates that there are four retired key management keys on the card (one 1024-bit RSA key and three 2048-bit RSA keys) and that the corresponding certificates for all four retired keys are also stored on the card. No URL is provided to obtain the retired certificates for key management from an off-

card source. Test PIV Card 3 supports secure messaging using cipher suite 2 and also implements the VCI. The Secure Messaging Certificate Signer data object includes an Intermediate Card Verifiable Certificate (CVC) along with a content signer certificate that has an RSA subject public key.

Test PIV Card 4:

All of the current certificates and data objects on Test PIV Card 4 are signed using ECDSA (Curve P-256) with SHA-256, and all of the current certificates on the card contain ECC Curve P-256 subject public keys.[3] The PIV Authentication certificate includes a UPN in the subjectAltName extension. Test PIV Card 4 includes a Discovery object that indicates that the Global PIN may be used to unlock the PIV Card Application but that the PIV Card Application PIN is the primary PIN used to unlock the PIV Card Application. Finally, Test PIV Card 4 includes a Key History object that indicates that there are nine retired key management keys on the card (three 2048-bit RSA keys and six ECC Curve P-256 keys) and that the certificates corresponding to seven of the keys are also stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 4 supports secure messaging using cipher suite 2 and also implements the VCI.

Test PIV Card 5:

All of the current certificates and data objects on Test PIV Card 5 are signed using ECDSA (Curve P-384) with SHA-384. The digital signature and key management keys on Test PIV Card 5 are ECC Curve P-384, while the PIV Authentication and Card Authentication keys are ECC Curve P-256. Like the PIV Authentication certificate on Test PIV Card 2, the PIV Authentication certificate on Test PIV Card 5 does not include any name forms in the subjectAltName extension other than the FASC-N and the UUID. Test PIV Card 5 includes a Key History object that indicates that there are six retired key management keys on the card (two 2048-bit RSA, two ECC Curve P-256, two ECC Curve P-384) but that none of the corresponding certificates are stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 5 supports secure messaging using cipher suite 7 and also implements the VCI.

Test PIV Card 6:

Test PIV Card 6 only contains those data objects that are listed as mandatory in [SP800-73] (except for the Discovery object and Biometric Information Templates Group Template, which are present on every test card).[4] Test PIV Card 6 includes a PIV Authentication certificate and a Card Authentication certificate but no digital signature certificate or key management certificate. The subject name in the PIV Authentication certificate contains the card's FASC-N rather than the cardholder's name, and the subjectAltName extension in the

[3] A few of the retired certificates for key management contain RSA subject public keys and are signed using RSA PKCS #1 v1.5.
[4] The BIT Group Template on every test card except Test PIV Card 8 contains no BITs, indicating that on-card biometric comparison is not supported.

PIV Authentication certificate only includes the card's FASC- N and UUID. The card's FASC-N indicates that the cardholder is a contractor, and the NACI indicator extension in the PIV Authentication certificate indicates that the cardholder's NACI had not been completed at the time that the certificate was issued. The Printed Information buffer is not present on the card.

Test PIV Card 7:

Test PIV Card 7 represents a legacy PIV Card. Unlike all of the other test cards, the PIV Authentication, digital signature, and key management certificates on Test PIV Card 7 do not include an extended key usage extension. Like Test PIV Card 1, the PIV Authentication certificate on Test PIV Card 7 includes a UPN in the subjectAltName. Test PIV Card 7 is the only card other than Test PIV Card 3 that includes a Discovery object that indicates that the Global PIN is the primary PIN to unlock the PIV Card Application. Test PIV Card 7 also includes a Key History object that indicates that there are six retired key management keys on the card (one 1024-bit RSA key and five 2048-bit RSA keys) and that the certificates corresponding to four of these keys are stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 7 does not support secure messaging.

Test PIV Card 8:

The PIV Authentication, Card Authentication, digital signature, and key management certificates on Test PIV Card 8 contain long serial numbers (up to 20 octets). The PIV Authentication certificate includes a UPN. The NACI indicator extension in the PIV Authentication and Card Authentication certificates indicates that the cardholder's NACI had not been completed at the time that the certificate was issued. Test PIV Card 8 includes a Discovery object that indicates that the Global PIN may be used to unlock the PIV Card Application but that the PIV Card Application PIN is the primary PIN used to unlock the PIV Card Application. Test PIV Card 8 includes a Key History object that indicates that there are 20 retired key management keys on the card (two 1024-bit RSA, fourteen 2048-bit RSA, two ECC Curve P-256, and two ECC Curve P-384) and that the certificates corresponding to all 20 of these keys are stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 8 also represents a scenario in which the cardholder's name has changed, and so the subject name and email address in some of the older, retired certificates for key management are different than in the cardholder's current certificates. Test PIV Card 8 is the only card in the set that supports OCC. Test PIV Card 8 supports secure messaging using cipher suite 7, allowing the card to support the OCC-AUTH authentication mechanism from Appendix B.1.4 of SP 800-73-4, Part 1. Test PIV Card 8 does not implement the VCI.

Test PIV Card 9:

Test PIV Card 9 is similar to Test PIV Card 1 except that Test PIV Card 9 is expired. Test PIV Card 9 is a short-term card that was issued to a contractor whose NACI had not been completed at the time that the certificates on the card were issued.

Test PIV Card 10:

Test PIV Card 10 represents a card that has been reported as lost. The PIV Authentication, Card Authentication, digital signature, and key management certificates have all been revoked with a reason code of key compromise. Test PIV Card 10 includes a Key History object that indicates that there are six retired key management keys on the card (all 2048-bit RSA keys) and that the certificates corresponding to two of these keys are stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 10 supports secure messaging using cipher suite 7 and also implements the VCI.

Test PIV Card 11:

Test PIV Card 11 represents a card that was created by an adversary in order to attempt to impersonate the holder of Test PIV Card 1. None of the signatures on any of the certificates or data objects are valid. The certificates on Test PIV Card 11 are identical to the certificates on Test PIV Card 1, except that the subject public keys correspond to the private keys that are on Test PIV Card 11. The biometric data (fingerprints and facial image) are those of the adversary.

Test PIV Card 12:

Test PIV Card 12 represents a PIV Card that was legitimately issued but where the cardholder has managed to replace the CHUID on the card with the CHUID from Test PIV Card 1 while leaving all of the other data objects on the card unchanged. This means that all of the data objects on the card are valid, but the FASC-N and GUID in the CHUID do not match the FASC-N and UUID in the biometric data objects or in the authentication certificates. If PIV biometric authentication was performed as specified in Section 6.2.1.1 of [FIPS201], but the check to verify that the FASC- N in the fingerprint data object matched the FASC-N in the CHUID data object was skipped, then the holder of Test PIV Card 12 could authenticate as the holder of Test PIV Card 1. Test PIV Card 12 supports secure messaging using cipher suite 2 and also implements the VCI.

Test PIV Card 13:

On Test PIV Card 13, the card has not expired, but the PIV Authentication, Card Authentication, digital signature, and key management certificates have expired.

Test PIV Card 14:

On Test PIV Card 14, the certificate that corresponds to the private key used to sign the CHUID, Security object, and biometric data objects on the card has been revoked with a revocation reason of key compromise. The cardholder's certificates are valid. Test PIV Card 14 includes a Key History object that indicates that there are seven retired key management keys on the card (all 2048-bit RSA) and that the certificates corresponding to three of the keys are stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 14 supports secure messaging using cipher suite 7 and also implements the VCI.

Test PIV Card 15:

Like Test PIV Card 10, Test PIV Card 15 also represents a card that has been reported as lost. On Test PIV Card 15, however, all of the current certificates and data objects have been signed using ECDSA (Curve P-256) with SHA-256, and all of the cardholder's current certificates contain ECC Curve P-256 subject public keys. The PIV Authentication, Card Authentication, digital signature, and key management certificates have been revoked with a revocation reason of key compromise. Test PIV Card 15 includes a Key History object that indicates that there are seven retired key management keys on the card (one 1024-bit RSA, two 2048-bit RSA, and four ECC Curve P-256) and that the certificates corresponding to five of these keys are stored on the card. A URL is provided that refers to a file containing all of the retired certificates for key management. Test PIV Card 15 supports secure messaging using cipher suite 2 and also implements the VCI.

Test PIV Card 16:

Test PIV-I Card 16 represents a PIV-I Card rather than a PIV Card. The FASC-N data element of the CHUID contains a value that indicates that the card is a PIV-I card. The FASC-N is not included in the signed data objects or in the authentication certificates. Test PIV-I Card 16 supports secure messaging using cipher suite 7. As with Test PIV Card 3, the Secure Messaging Certificate Signer data object includes an Intermediate Card Verifiable Certificate (CVC) along with a content signer certificate that has an RSA subject public key.

References

[COMMON] Federal PKI Certificate Policy Authority (2020) Common Policy X.509 Certificate and Certificate Revocation List (CRL) Profiles. Available at: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profile-common.pdf

[FIPS201] National Institute of Standards and Technology (2013) Personal Identity Verification (PIV) of Federal Employees and Contractors. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 201-2. https://doi.org/10.6028/NIST.FIPS.201-2

[NISTIR7870] Cooper DA (2012) NIST Test Personal Identity Verification (PIV) Cards. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Interagency or Internal Report (IR) 7870. https://doi.org/10.6028/NIST.IR.7870

[PIV-I] Federal PKI Certificate Policy Authority (2018) X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification Interoperable (PIV-I) Cards. Available at: https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-x509-cert-profiles-pivi.pdf

[RFC4556] Zhu L, Tung B (2006) Public Key Cryptography for Initial Authentication in Kerberos (PKINIT). (Internet Engineering Task Force (IETF) Network Working Group), IETF Request for Comments (RFC) 4556. https://doi.org/10.17487/RFC4556

[SP800-73] Cooper DA, Ferraiolo H, Mehta KL, Francomacaro S, Chandramouli R, Mohler J (2015) Interfaces for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-73-4, Includes updates as of February 8, 2016. https://doi.org/10.6028/NIST.SP.800-73-4

[SP800-76] Grother PJ, Salamon WJ, Chandramouli R (2013) Biometric Specifications for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-76-2. https://doi.org/10.6028/NIST.SP.800-76-2

[SP800-78] Polk WT, Dodson DF, Burr WE, Ferraiolo H, Cooper DA (2015) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) 800-78-4. https://doi.org/10.6028/NIST.SP.800-78-4

Appendix A—Acronyms

Selected acronyms and abbreviations used in this paper are defined below.

APDU	Application Protocol Data Unit
CA	Certification Authority
CHUID	Card Holder Unique Identifier
CRL	Certificate Revocation List
CVC	Card Verifiable Certificate
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
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
IETF	Internet Engineering Task Force
LDAP	Lightweight Directory Access Protocol
NACI	National Agency Check with Inquiries
NIST	National Institute of Standards and Technology
OCC	On-card Biometric Comparison
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PIN	Personal Identification Number
PIV	Personal Identity Verification
PKCS	Public-Key Cryptography Standards

PUK	PIN Unblocking Key
RFC	Request for Comments
RSA	Rivest, Shamir, Adleman cryptographic algorithm
RSASSA-PSS	RSA Signature Scheme with Appendix – Probabilistic Signature Scheme
SHA	Secure Hash Algorithm
SM	Secure Messaging
SO	Security Object
SP	Special Publication
TLS	Transport Layer Security
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
UUID	Universally Unique Identifier
VCI	Virtual Contact Interface

Appendix B—Test Card PIN Values

The second and third columns of Table 1 list 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. The fourth column of Table 1 lists the pairing code values for each card that implements the virtual contact interface (VCI). The PIN Unblocking Key (PUK) for all 16 cards is 99999999.

Table 1 - Test Card PIN Values

Card	PIV Card Application PIN	Global PIN	Pairing Code
Test PIV Card 1	**123456**		
Test PIV Card 2	**123456**		00000002
Test PIV Card 3	90909090	**111111**	00000003
Test PIV Card 4	**123456**	12345678	00000004
Test PIV Card 5	**123456**		00000005
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**		00000010
Test PIV Card 11	**123456**		
Test PIV Card 12	**123456**		00000012
Test PIV Card 13	**123456**		
Test PIV Card 14	**123456**		00000014
Test PIV Card 15	**123456**		00000015
Test PIV-I Card 16	**123456**		00000016

Appendix C—Test Card Details

Table 2 provides a brief summary of the contents of each of the test cards. The following subsections provide detailed information on the contents of each card.

Table 2 - Summary of Test Card Contents

#	Cardholder Certificates	Certificate Signatures	Certificate Status	CHUID/SO Signatures	Biometric Signatures	Discovery Object and SM
1	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN, OCC, or VCI. No SM
2	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 3072 bit RSASSA-PSS with SHA-256	Valid	RSA 3072 bit RSASSA-PSS with SHA-256	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 7
3	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 4096 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256	RSA 4096 bit PKCS #1 v1.5 with SHA-256	Global PIN is primary. No OCC. VCI implemented. SM: Cipher suite 2
4	9A: ECC P-256 9C: ECC P-256 9D: ECC P-256 9E: ECC P-256	ECDSA with SHA-256, Curve P-256	Valid	ECDSA with SHA-256, Curve P-256	Same signer as CHUID/SO	Global PIN present, but not primary. No OCC. VCI implemented. SM: Cipher suite 2
5	9A: ECC P-256 9C: ECC P-384 9D: ECC P-384 9E: ECC P-256	ECDSA with SHA-384, Curve P-384	Valid	ECDSA with SHA-384, Curve P-384	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 7
6	9A: RSA 2048 bit 9C: not present 9D: not present 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN, OCC, or VCI. No SM
7	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	Global PIN is primary. No OCC or VCI. No SM
8	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 4096 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	Global PIN present, but not primary. OCC implemented. No VCI. SM: Cipher suite 7

#	Cardholder Certificates	Certificate Signatures	Certificate Status	CHUID/SO Signatures	Biometric Signatures	Discovery Object and SM
9	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Expired	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN, OCC, or VCI. No SM
10	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Revoked	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 7
11	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Invalid signatures	RSA 2048 bit PKCS #1 v1.5 with SHA-256 (invalid signatures)	Same signer as CHUID/SO	No Global PIN, OCC, or VCI. No SM
12	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 2
13	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Expired	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN, OCC, or VCI. No SM
14	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256 (revoked certificate)	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 7
15	9A: ECC P-256 9C: ECC P-256 9D: ECC P-256 9E: ECC P-256	ECDSA with SHA-256, Curve P-256	Revoked	ECDSA with SHA-256, Curve P-256	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 2
16	9A: RSA 2048 bit 9C: RSA 2048 bit 9D: RSA 2048 bit 9E: RSA 2048 bit	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Valid	RSA 2048 bit PKCS #1 v1.5 with SHA-256	Same signer as CHUID/SO	No Global PIN or OCC. VCI implemented. SM: Cipher suite 7

C.1 Test PIV Card 1

Discovery Object:

PIN Usage Policy: 0x40 0x00 (no Global PIN, OCC, or VCI)

CHUID:

FASC-N: D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED
(Agency Code = 3201, System Code = 0295, Credential Number = 834563, CS = 1, ICI = 2, PI = 6464979587, OC = 1, OI = 3201, POA = 1)

Buffer Length: not present

GUID: 26092f20-f792-4f7f-94b2-d0923cce6c7a

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates: (GZIP compressed)

- Test PIV Card 1: PIV Authentication Certificate
- Test PIV Card 1: Card Authentication Certificate
- Test PIV Card 1: Digital Signature Certificate
- Test PIV Card 1: Key Management Certificate
- Test PIV Card 1: Retired Key Management Certificate A

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

Printed Information:

Name: Test Cardholder

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212345

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Not supported

C.2 Test PIV Card 2

Discovery Object:

PIN Usage Policy: 0x48 0x00 (no Global PIN or OCC. VCI is implemented)

CHUID:

FASC-N: D6501858289D6C1C92ADE58360D8210842108421084210842108421087E4
(Agency Code = 3201, System Code = 0295, Credential Number = 034567, CS = 0, ICI = 0, PI = 0000000000, OC = 0, OI = 0000, POA = 0)

Buffer Length: not present

GUID: 44be5385-2e86-434d-b45e-b3e09fcc0dca

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates: (GZIP compressed)

- Test PIV Card 2: PIV Authentication Certificate
- Test PIV Card 2: Card Authentication Certificate
- Test PIV Card 2: Digital Signature Certificate
- Test PIV Card 2: Key Management Certificate
- Test PIV Card 2: Retired Key Management Certificate A

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

Printed Information:

Name: Test Cardholder Jr.

Issuer Identification: TSTISR320161719

Employee Affiliation: Contractor

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212346

Cardholder Fingerprints:

Indicator that no fingerprints could be obtained for the cardholder.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

Biometric Data Objects: RSASSA-PSS with SHA-256, signed by PIV Content Signer 2

Secure Messaging:

Cipher Suite 7

X.509 Certificate for Content Signing: PIV Content Signer 4 (GZIP compressed)

Intermediate CVC: not present

C.3 Test PIV Card 3

Discovery Object:

PIN Usage Policy: 0x68 0x20 (Global PIN is present and is the primary PIN. No OCC. VCI is implemented)

CHUID:

FASC-N: D650185855E56DC8127945A16CDB906E7880C08286501843F5
(Agency Code = 3201, System Code = 8575, Credential Number = 714932, CS=1, ICI=3, PI=7163720148, OC=1, OI=3201, POA=1)

Buffer Length: present

GUID: 45853470-a403-4844-ae15-c6495959fad5

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: 0aaa9975-f233-4e9a-98e4-faf7e103e96c

Cardholder Certificates:

- Test PIV Card 3: PIV Authentication Certificate
- Test PIV Card 3: Card Authentication Certificate
- Test PIV Card 3: Digital Signature Certificate
- Test PIV Card 3: Key Management Certificate
- Test PIV Card 3: Retired Key Management Certificate A
- Test PIV Card 3: Retired Key Management Certificate B
- Test PIV Card 3: Retired Key Management Certificate C
- Test PIV Card 3: Retired Key Management Certificate D

Key History Object:

keysWithOnCardCerts = 4, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

Printed Information:

Name: Test Cardholder III

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212347

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects but not CHUID.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 5

Secure Messaging:

Cipher Suite 2

X.509 Certificate for Content Signing: PIV Content Signer 1

Intermediate CVC: present

C.4 Test PIV Card 4

Discovery Object:

PIN Usage Policy: 0x68 0x10 (Global PIN is present but is not the primary PIN. No OCC. VCI is implemented)

CHUID:

FASC-N: D650185B3CCE6D9C905325A1625A10AA09C4378486501843EB
(Agency Code = 3201, System Code = 3733, Credential Number = 334894, CS=1, ICI=4, PI=1152472674, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: a4eb5a09-66c3-4f3e-83f3-b77e0ee96a25

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: c1471a8d-11bd-4053-813f-0b04aa7be78b

Cardholder Certificates:

- Test PIV Card 4: PIV Authentication Certificate
- Test PIV Card 4: Card Authentication Certificate
- Test PIV Card 4: Digital Signature Certificate
- Test PIV Card 4: Key Management Certificate
- Test PIV Card 4: Retired Key Management Certificate A
- Test PIV Card 4: Retired Key Management Certificate B
- Test PIV Card 4: Retired Key Management Certificate C
- Test PIV Card 4: Retired Key Management Certificate D
- Test PIV Card 4: Retired Key Management Certificate E
- Test PIV Card 4: Retired Key Management Certificate F
- Test PIV Card 4: Retired Key Management Certificate G
- Test PIV Card 4: Retired Key Management Certificate H
- Test PIV Card 4: Retired Key Management Certificate I

Key History Object:

keysWithOnCardCerts = 7, *keysWithOffCardCerts* = 2, *offCardCertURL*:
http://smime2.nist.gov/86D8D563F12E91D07B7EC367F160D69BB15AB330618EAC314A4A81D28FD11F0

Printed Information:

Name: Test Cardholder IV

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212348

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects but not CHUID.

Data Object Signatures:

CHUID and Security Object: ECDSA with SHA-256, signed by PIV Content Signer 3

Biometric Data Objects: ECDSA with SHA-256, signed by PIV Content Signer 3

Secure Messaging:

Cipher Suite 2, X.509 Certificate for Content Signing: PIV Content Signer 3, Intermediate CVC: not present

C.5 Test PIV Card 5

Discovery Object:

PIN Usage Policy: 0x48 0x00 (No Global PIN or OCC. VCI is implemented)

CHUID:

FASC-N: D650185A13422C2267930D9162589080501E649C86501843FC
(Agency Code = 3201, System Code = 1922, Credential Number = 843790, CS=2, ICI=4, PI=4110207347, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: be694761-f813-46cb-9d3a-28a0142f98e6

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 5: PIV Authentication Certificate
- Test PIV Card 5: Card Authentication Certificate
- Test PIV Card 5: Digital Signature Certificate
- Test PIV Card 5: Key Management Certificate
- Test PIV Card 5: Retired Key Management Certificate A
- Test PIV Card 5: Retired Key Management Certificate B
- Test PIV Card 5: Retired Key Management Certificate C
- Test PIV Card 5: Retired Key Management Certificate D
- Test PIV Card 5: Retired Key Management Certificate E
- Test PIV Card 5: Retired Key Management Certificate F

Key History Object:

keysWithOnCardCerts = 0, *keysWithOffCardCerts* = 6, *offCardCertURL*:
http://smime2.nist.gov/124571D80DCDB4087C11D85C54EE4B9540E481CADCB7F44736DDDD6201C799D3

Printed Information:

Name: Test Cardholder V

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212349

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes unsigned data objects but not CHUID, Cardholder Fingerprints, or Cardholder Facial Image.

Data Object Signatures:

CHUID and Security Object: ECDSA with SHA-384, signed by PIV Content Signer 4

Biometric Data Objects: ECDSA with SHA-384, signed by PIV Content Signer 4

Secure Messaging:

Cipher Suite 7

X.509 Certificate for Content Signing: PIV Content Signer 4, Intermediate CVC: not present

C.6 Test PIV Card 6

Discovery Object:

PIN Usage Policy: 0x40 0x00 (no Global PIN, OCC, or VCI)

CHUID:

FASC-N: D65018582214EC29D72125A1645899207990B49086501857E1
(Agency Code = 3201, System Code = 0889, Credential Number = 895304, CS=1, ICI=2, PI=4340730641, OC=1, OI=3201, POA=5)

Buffer Length: not present

GUID: 0a40b578-723f-42c8-9923-09ecd0163d6a

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 6: PIV Authentication Certificate
- Test PIV Card 6: Card Authentication Certificate

Key History Object:

Not present

Printed Information:

Not present

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes unsigned data objects but not CHUID, Cardholder Fingerprints, or Cardholder Facial Image.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Not supported

C.7 Test PIV Card 7

Discovery Object:

PIN Usage Policy: 0x60 0x20 (Global PIN is present and is the primary PIN. No OCC or VCI)

CHUID:

FASC-N: D650185A1C84EC10850D6DA16E5B958121C0B61C86501843E8
(Agency Code = 3201, System Code = 1719, Credential Number = 000266, CS=1, ICI=7, PI=7514170617, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: 9a4b12d1-d28c-498c-8182-37875ac7a0c4

Organizational Identifier: 3201

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 7: PIV Authentication Certificate
- Test PIV Card 7: Card Authentication Certificate
- Test PIV Card 7: Digital Signature Certificate
- Test PIV Card 7: Key Management Certificate
- Test PIV Card 7: Retired Key Management Certificate A
- Test PIV Card 7: Retired Key Management Certificate B
- Test PIV Card 7: Retired Key Management Certificate C
- Test PIV Card 7: Retired Key Management Certificate D
- Test PIV Card 7: Retired Key Management Certificate E
- Test PIV Card 7: Retired Key Management Certificate F

Key History Object:

keysWithOnCardCerts = 4, *keysWithOffCardCerts* = 2, *offCardCertURL*:
http://smime2.nist.gov/C78DAAAB0B551D7CB5C78DE8A39A80ADE560B4FD2A9DD4374E980B6988F2CC46

Printed Information:

Name: Test Cardholder VII

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Test Department

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212351

Cardholder Fingerprints:

Right index finger from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Not supported

C.8 Test PIV Card 8

Discovery Object:

PIN Usage Policy: 0x70 0x10 (Global PIN is present but is not the primary PIN. OCC is implemented. No VCI.)

CHUID:

FASC-N: D6501859ADA92C1E5602E5A169DB9545450692B086501843ED
(Agency Code = 3201, System Code = 6654, Credential Number = 075187, CS=1, ICI=9, PI=7525816451, OC=1, OI=3201, POA=1)

Buffer Length: present

GUID: 12b9c2c3-8e0e-4cbe-a0d1-fc906174bb94

Organizational Identifier: 3201

Expiration Data: 20401231

DUNS: 362288719

Cardholder UUID: eb0d8081-cd7e-4f1d-9e50-8ccfd0c94df4

Cardholder Certificates:

- Test PIV Card 8: PIV Authentication Certificate
- Test PIV Card 8: Card Authentication Certificate
- Test PIV Card 8: Digital Signature Certificate
- Test PIV Card 8: Key Management Certificate
- Test PIV Card 8: Retired Key Management Certificate A
- Test PIV Card 8: Retired Key Management Certificate B
- Test PIV Card 8: Retired Key Management Certificate C
- Test PIV Card 8: Retired Key Management Certificate D
- Test PIV Card 8: Retired Key Management Certificate E
- Test PIV Card 8: Retired Key Management Certificate F
- Test PIV Card 8: Retired Key Management Certificate G
- Test PIV Card 8: Retired Key Management Certificate H
- Test PIV Card 8: Retired Key Management Certificate I
- Test PIV Card 8: Retired Key Management Certificate J
- Test PIV Card 8: Retired Key Management Certificate K
- Test PIV Card 8: Retired Key Management Certificate L
- Test PIV Card 8: Retired Key Management Certificate M
- Test PIV Card 8: Retired Key Management Certificate N
- Test PIV Card 8: Retired Key Management Certificate O
- Test PIV Card 8: Retired Key Management Certificate P
- Test PIV Card 8: Retired Key Management Certificate Q
- Test PIV Card 8: Retired Key Management Certificate R
- Test PIV Card 8: Retired Key Management Certificate S
- Test PIV Card 8: Retired Key Management Certificate T

Key History Object:

keysWithOnCardCerts = 20, *keysWithOffCardCerts* = 0, *offCardCertURL*:
http://smime2.nist.gov/C86D3B153626C22DBE275FB458C1CE9C655080C26CCB834AADA63C4100527800

Printed Information:

Name: Test Cardholder VIII

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Test

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Department

Agency Card Serial Number: 0000212352

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Left and right middle fingers from Figure 2.

Security Object:

Includes Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects but not CHUID.

Data Object Signatures:

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

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 5

Secure Messaging:

Cipher Suite 7

X.509 Certificate for Content Signing: PIV Content Signer 4

Intermediate CVC: not present

C.9 Test PIV Card 9

Discovery Object:

PIN Usage Policy: 0x40 0x00 (no Global PIN, OCC, or VCI)

CHUID:

FASC-N: D650185AA4412D084E750DA164590826784E204886501857FC
(Agency Code = 3201, System Code = 5424, Credential Number = 119950, CS=1, ICI=2, PI=2243747282, OC=1, OI=3201, POA=5)

Buffer Length: not present

GUID: 6a7c77e2-933d-4e40-84b6-6c903ae8d220

Organizational Identifier: not present

Expiration Data: 20200405

DUNS: not present

Cardholder UUID: 04927918-e9f3-4baf-8612-f2e0a8ad7506

Cardholder Certificates: (GZIP compressed)

- Test PIV Card 9: PIV Authentication Certificate
- Test PIV Card 9: Card Authentication Certificate
- Test PIV Card 9: Digital Signature Certificate
- Test PIV Card 9: Key Management Certificate
- Test PIV Card 9: Retired Key Management Certificate A

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

Printed Information:

Name: Test Cardholder IX

Issuer Identification: TSTISR320161719

Employee Affiliation: Contractor

Organization Affiliation (Line 1): Not present

Expiration Date: 2020APR05

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212353

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Not supported

C.10 Test PIV Card 10

Discovery Object:

PIN Usage Policy: 0x48 0x00 (no Global PIN or OCC. VCI is implemented)

CHUID:

FASC-N: D650185A0D412D5AB4999DA1625A75257286D6B086501843EE
(Agency Code = 3201, System Code = 1624, Credential Number = 556439, CS=1, ICI=4, PI=9545326551, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: 0375b685-f108-4df7-8dec-3a11ec525c6f

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 10: PIV Authentication Certificate
- Test PIV Card 10: Card Authentication Certificate
- Test PIV Card 10: Digital Signature Certificate
- Test PIV Card 10: Key Management Certificate
- Test PIV Card 10: Retired Key Management Certificate A
- Test PIV Card 10: Retired Key Management Certificate B
- Test PIV Card 10: Retired Key Management Certificate C
- Test PIV Card 10: Retired Key Management Certificate D
- Test PIV Card 10: Retired Key Management Certificate E
- Test PIV Card 10: Retired Key Management Certificate F

Key History Object:

keysWithOnCardCerts = 2, *keysWithOffCardCerts* = 4, *offCardCertURL*:
http://smime2.nist.gov/5246BEC8227FE7C9F646AEF347A1AA075E258D4A5748E38AA6FF04BA8C513158

Printed Information:

Name: Test Cardholder X

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): not present

Agency Card Serial Number: 0000212354

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Cipher Suite 7

X.509 Certificate for Content Signing: PIV Content Signer 4, Intermediate CVC: not present

C.11 Test PIV Card 11

Discovery Object:

PIN Usage Policy: 0x40 0x00 (no Global PIN, OCC, or VCI)

CHUID:

FASC-N: D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED
(Agency Code = 3201, System Code = 0295, Credential Number = 834563, CS = 1, ICI = 2, PI = 6464979587, OC = 1, OI = 3201, POA = 1)

Buffer Length: not present

GUID: 26092f20-f792-4f7f-94b2-d0923cce6c7a

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates: (GZIP compressed)

- Test PIV Card 11: PIV Authentication Certificate
- Test PIV Card 11: Card Authentication Certificate
- Test PIV Card 11: Digital Signature Certificate
- Test PIV Card 11: Key Management Certificate

Key History Object:

Not present

Printed Information:

Name: Test Cardholder

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 2170336744

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1. Signature is invalid.

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1. Signature is invalid.

Secure Messaging:

Not supported

C.12 Test PIV Card 12

Discovery Object:

PIN Usage Policy: 0x48 0x00 (no Global PIN or OCC. VCI is implemented)

CHUID:[5]

FASC-N: D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED
(Agency Code = 3201, System Code = 0295, Credential Number = 834563, CS = 1, ICI = 2, PI = 6464979587, OC = 1, OI = 3201, POA = 1)

Buffer Length: not present

GUID: 26092f20-f792-4f7f-94b2-d0923cce6c7a

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates: (GZIP compressed)

- Test PIV Card 12: PIV Authentication Certificate
- Test PIV Card 12: Card Authentication Certificate
- Test PIV Card 12: Digital Signature Certificate
- Test PIV Card 12: Key Management Certificate
- Test PIV Card 12: Retired Key Management Certificate A

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

Printed Information:

Name: Test Cardholder XII

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212355

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects but not CHUID.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Cipher Suite 2

X.509 Certificate for Content Signing: PIV Content Signer 3 (GZIP compressed), Intermediate CVC: not present

[5] Note that the CHUID on Test PIV Card 12 was copied from Test PIV Card 1, and so the FASC-N and GUID in the CHUID do not match the FASC-N and UUID that appear in the cardholder's certificates and biometric data objects.

C.13 Test PIV Card 13

Discovery Object:

PIN Usage Policy: 0x40 0x00 (no Global PIN, OCC, or VCI)

CHUID:

FASC-N: D6501859019B6D0E708D6DA164585324D042221586501843EB
(Agency Code = 3201, System Code = 2096, Credential Number = 177466, CS=1, ICI=2, PI=8949244215, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: af6a1130-2635-43ac-9c89-175e062b1343

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 13: PIV Authentication Certificate
- Test PIV Card 13: Card Authentication Certificate
- Test PIV Card 13: Digital Signature Certificate
- Test PIV Card 13: Key Management Certificate
- Test PIV Card 13: Retired Key Management Certificate A

Key History Object:

keysWithOnCardCerts = 1, *keysWithOffCardCerts* = 0, *offCardCertURL* not present

Printed Information:

Name: Test Cardholder III

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212356

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 1

Secure Messaging:

Not supported

C.14 Test PIV Card 14

Discovery Object:

PIN Usage Policy: 0x48 0x00 (no Global PIN or OCC. VCI is implemented)

CHUID:

FASC-N: D6501858999CED9992150DA166D9A19C279A844486501843EE
(Agency Code = 3201, System Code = 4399, Credential Number = 394150, CS=1, ICI=6, PI=6091935084, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: 71417603-ef9b-4651-812a-d023c8f8d592

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates: (GZIP compressed)

- Test PIV Card 14: PIV Authentication Certificate
- Test PIV Card 14: Card Authentication Certificate
- Test PIV Card 14: Digital Signature Certificate
- Test PIV Card 14: Key Management Certificate
- Test PIV Card 14: Retired Key Management Certificate A
- Test PIV Card 14: Retired Key Management Certificate B
- Test PIV Card 14: Retired Key Management Certificate C
- Test PIV Card 14: Retired Key Management Certificate D
- Test PIV Card 14: Retired Key Management Certificate E
- Test PIV Card 14: Retired Key Management Certificate F
- Test PIV Card 14: Retired Key Management Certificate G

Key History Object:

keysWithOnCardCerts = 3, *keysWithOffCardCerts* = 4, *offCardCertURL*:
http://smime2.nist.gov/39AB5D2D413D018F73938D4BEB0C0C7606DA027C1D885F908E343F8A55532164

Printed Information:

Name: Test Cardholder XIV

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212357

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 6

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV Content Signer 6

Secure Messaging:

Cipher Suite 7

X.509 Certificate for Content Signing: PIV Content Signer 4 (GZIP compressed), Intermediate CVC: not present

C.15 Test PIV Card 15

Discovery Object:

PIN Usage Policy: 0x48 0x00 (no Global PIN or OCC. VCI is implemented)

CHUID:

FASC-N: D65018591C422CD9E51CE5A16ADB88241A49E5A486501843E7
(Agency Code = 3201, System Code = 2722, Credential Number = 693277, CS=1, ICI=5, PI=7241649364, OC=1, OI=3201, POA=1)

Buffer Length: not present

GUID: 6c4ecd74-88c4-4828-9521-4902c8b4687c

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: not present

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 15: PIV Authentication Certificate
- Test PIV Card 15: Card Authentication Certificate
- Test PIV Card 15: Digital Signature Certificate
- Test PIV Card 15: Key Management Certificate
- Test PIV Card 15: Retired Key Management Certificate A
- Test PIV Card 15: Retired Key Management Certificate B
- Test PIV Card 15: Retired Key Management Certificate C
- Test PIV Card 15: Retired Key Management Certificate D
- Test PIV Card 15: Retired Key Management Certificate E
- Test PIV Card 15: Retired Key Management Certificate F
- Test PIV Card 15: Retired Key Management Certificate G

Key History Object:

keysWithOnCardCerts = 5, *keysWithOffCardCerts* = 2, *offCardCertURL*:
http://smime2.nist.gov/E041C8D3CDD67ED269F977F174F1DD47493683AD100DBECE0E10422D106E4097

Printed Information:

Name: Test Cardholder XV

Issuer Identification: TSTISR320161719

Employee Affiliation: Employee

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212358

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: ECDSA with SHA-256, signed by PIV Content Signer 3

Biometric Data Objects: ECDSA with SHA-256, signed by PIV Content Signer 3

Secure Messaging:

Cipher Suite 2

X.509 Certificate for Content Signing: PIV Content Signer 3, Intermediate CVC: not present

C.16 Test PIV-I Card 16

Discovery Object:

PIN Usage Policy: 0x48 0x00 (no Global PIN or OCC. VCI is implemented)

CHUID:

FASC-N: D4E739DA739CED39CE739DA16459B398A798667986501837F0
(Agency Code = 9999, System Code = 9999, Credential Number = 999999, CS=1, ICI=2, PI=6998931393, OC=1, OI=3201, POA=6)

Buffer Length: not present

GUID: e51faf01-14d7-471d-83e1-69e5d725ba64

Organizational Identifier: not present

Expiration Data: 20401231

DUNS: 610796612

Cardholder UUID: not present

Cardholder Certificates:

- Test PIV Card 16: PIV Authentication Certificate
- Test PIV Card 16: Card Authentication Certificate
- Test PIV Card 16: Digital Signature Certificate
- Test PIV Card 16: Key Management Certificate

Key History Object:

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

Printed Information:

Name: Test Cardholder XVI

Issuer Identification: TSTISR320161719

Employee Affiliation: Affiliate

Organization Affiliation (Line 1): Not present

Expiration Date: 2040DEC31

Organization Affiliation (Line 2): Not present

Agency Card Serial Number: 0000212359

Cardholder Fingerprints:

Left and right index fingers from Figure 2.

Biometric Information Templates Group Template:

Not present

Security Object:

Includes CHUID, Cardholder Fingerprints, Cardholder Facial Image, and unsigned data objects.

Data Object Signatures:

CHUID and Security Object: RSA PKCS #1 with SHA-256, signed by PIV-I Content Signer 1

Biometric Data Objects: RSA PKCS #1 with SHA-256, signed by PIV-I Content Signer 1

Secure Messaging:

Cipher Suite 7

X.509 Certificate for Content Signing: PIV-I Content Signer 1

Intermediate CVC: present

Appendix D—Certificate Details

D.1 CA Certificates

D.1.1 Self-Signed Trust Anchor Certificate

Serial Number: 1
Signature Algorithm: sha384WithRSAEncryption
Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US
Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT
Subject: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US
Subject Public Key Info: rsaEncryption, 4096-bit modulus, e=65537
Extensions:

Subject Key Identifier:
84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Key Usage: critical
Certificate Sign, CRL Sign

Basic Constraints: critical
CA:TRUE

Subject Information Access:
CA Repository - http://smime2.nist.gov/PIVTest2/CACertsIssuedByTrustAnchor.p7c
CA Repository - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

D.1.2 RSA 2048 Issuing CA Certificate

Serial Number: 2

Signature Algorithm: sha384WithRSAEncryption

Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Key Usage: critical

Certificate Sign, CRL Sign

Basic Constraints: critical

CA:TRUE, pathlen:0

Authority Key Identifier:

84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Subject Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Certificate Policies:

id_fpki_common_policy
id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning
id_fpki_common_dervied_pivAuth

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/TrustAnchor.crl

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToTrustAnchor.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

D.1.3 RSA 3072 Issuing CA Certificate

Serial Number: 3

Signature Algorithm: sha384WithRSAEncryption

Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test RSA 3072-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 3072-bit modulus, e=65537

Extensions:

Key Usage: critical

Certificate Sign, CRL Sign

Basic Constraints: critical

CA:TRUE, pathlen:0

Authority Key Identifier:

84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Subject Key Identifier:

9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Certificate Policies:

id_fpki_common_policy
id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning
id_fpki_common_dervied_pivAuth

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/TrustAnchor.crl

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToTrustAnchor.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

D.1.4 RSA 4096 Issuing CA Certificate

Serial Number: 8

Signature Algorithm: sha512WithRSAEncryption

Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test RSA 4096-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 4096-bit modulus, e=65537

Extensions:

Key Usage: critical

Certificate Sign, CRL Sign

Basic Constraints: critical

CA:TRUE, pathlen:0

Authority Key Identifier:

84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Subject Key Identifier:

0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Certificate Policies:

id_fpki_common_policy
id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning
id_fpki_common_dervied_pivAuth

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/TrustAnchor.crl

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToTrustAnchor.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

D.1.5 ECC P-256 Issuing CA Certificate

Serial Number: 4

Signature Algorithm: sha384WithRSAEncryption

Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Key Usage: critical

Certificate Sign, CRL Sign

Basic Constraints: critical

CA:TRUE, pathlen:0

Authority Key Identifier:

84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Subject Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Certificate Policies:

id_fpki_common_policy
id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning
id_fpki_common_dervied_pivAuth

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/TrustAnchor.crl

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToTrustAnchor.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

D.1.6 ECC P-384 Issuing CA Certificate

Serial Number: 5

Signature Algorithm: sha512WithRSAEncryption

Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Key Usage: critical

Certificate Sign, CRL Sign

Basic Constraints: critical

CA:TRUE, pathlen:0

Authority Key Identifier:

84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Subject Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Certificate Policies:

id_fpki_common_policy
id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning
id_fpki_common_dervied_pivAuth

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/TrustAnchor.crl

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToTrustAnchor.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

D.1.7 RSA 2048 PIV-I Issuing CA Certificate

Serial Number: 7

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test Trust Anchor for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2010 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Key Usage: critical

Certificate Sign, CRL Sign

Basic Constraints: critical

CA:TRUE, pathlen:0

Authority Key Identifier:

84:35:BC:7D:0A:8B:0A:16:0F:35:5E:29:EF:A6:CC:29:26:CF:2F:DB

Subject Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/TrustAnchor.crl

ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToTrustAnchor.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20Trust%20Anchor%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

Certificate Policies:

id_fpki_certpcy_pivi_hardware
id_fpki_certpcy_pivi_cardAuth
id_fpki_certpcy_pivi_contentSigning

Policy Mappings:

id_fpki_certpcy_pivi_hardware:id_pivi_issuer_certpcy_hardware,
id_fpki_certpcy_pivi_cardAuth:id_pivi_issuer_certpcy_cardAuth,
id_fpki_certpcy_pivi_contentSigning:id_pivi_issuer_certpcy_contentSigning

Policy Constraints:

Require Explicit Policy:0, Inhibit Policy Mapping:0

Inhibit Any Policy: 0

D.2 Content Signer Certificates

D.2.1 PIV Content Signer 1

Status: not revoked

Serial Number: 1

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV Content Signer 1, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
9B:C5:E7:73:5F:14:EC:7F:42:BA:EF:42:CD:A7:38:D0:A6:AE:B5:71

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_content_signing

Certificate Policies:
id_fpki_common_piv_contentSigning

D.2.2 PIV Content Signer 2

Status: not revoked

Serial Number: 2

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: CN=Test RSA 3072-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV Content Signer 2, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 3072-bit modulus, e=65537

Extensions:

Authority Key Identifier:

9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Subject Key Identifier:

F2:C6:16:79:41:BA:A6:62:C2:A2:F1:C9:CF:26:94:D0:8E:EC:57:C5

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA3072IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA3072IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_piv_content_signing

Certificate Policies:

id_fpki_common_piv_contentSigning

D.2.3 PIV Content Signer 3

Status: not revoked

Serial Number: 3

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV Content Signer 3, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

19:05:97:6B:DD:CA:82:3D:30:C6:59:C7:38:46:65:D0:1F:5B:60:B8

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_piv_content_signing

Certificate Policies:

id_fpki_common_piv_contentSigning

D.2.4 PIV Content Signer 4

Status: not revoked

Serial Number: 4

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV Content Signer 4, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

B6:10:37:92:27:0F:BD:08:20:FC:D4:2D:6C:12:18:49:4B:4B:5F:1E

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_piv_content_signing

Certificate Policies:

id_fpki_common_piv_contentSigning

D.2.5 PIV Content Signer 5

Status: not revoked

Serial Number: 5

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 4096-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV Content Signer 5, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 4096-bit modulus, e=65537

Extensions:

Authority Key Identifier:
0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Subject Key Identifier:
52:E1:28:3A:61:EB:CD:C8:D7:62:DB:46:A4:32:1A:88:9F:16:7B:AB

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA4096IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA4096IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_content_signing

Certificate Policies:
id_fpki_common_piv_contentSigning

D.2.6 PIV Content Signer 6

Status: revoked

Serial Number: 6

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV Content Signer 6, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
7C:60:F4:1F:43:98:44:06:41:04:79:DD:D9:5E:00:48:93:2E:7E:36

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_content_signing

Certificate Policies:
id_fpki_common_piv_contentSigning

D.2.7 PIV-I Content Signer 1

Status: not revoked

Serial Number: 6

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test PIV-I Content Signer 1, ou=Test CA, o=Test Certificates 2020, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

Subject Key Identifier:

4C:C9:C7:B3:A4:F1:C8:3E:C1:0D:7C:93:26:3F:FA:E7:77:74:78:9F

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048PIV-IIssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048PIV-IIssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_fpki_pivi_content_signing

Certificate Policies:

id_pivi_issuer_certpcy_contentSigning

D.3 OCSP Responder Certificates

D.3.1 RSA 2048-bit CA OCSP Responder Certificate

Serial Number: x (short lifetime certificate rekeyed every 12 hours)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 2048-bit CA for Test PIV Cards v2

Validity: Not Before: Oct 20 14:00:00 2020 GMT, Not After: Oct 22 14:00:00 2020 GMT

Subject: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 2048-bit CA's OCSP Responder

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Key Usage: critical

Digital Signature

Extended Key Usage:

OCSP Signing

OCSP No Check:

Certificate Policies:

id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning

Subject Key Identifier:

SHA-1 hash of subject public key

D.3.2 RSA 3072-bit CA OCSP Responder Certificate

Serial Number: x (short lifetime certificate rekeyed every 12 hours)

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 3072-bit CA for Test PIV Cards v2

Validity: Not Before: Oct 20 14:00:01 2020 GMT, Not After: Oct 22 14:00:01 2020 GMT

Subject: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 3072-bit CA's OCSP Responder

Subject Public Key Info: rsaEncryption, 3072-bit modulus, e=65537

Extensions:

Authority Key Identifier:

9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Key Usage: critical

Digital Signature

Extended Key Usage:

OCSP Signing

OCSP No Check:

Certificate Policies:

id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning

Subject Key Identifier:

SHA-1 hash of subject public key

D.3.3 RSA 4096-bit CA OCSP Responder Certificate

Serial Number: x (short lifetime certificate rekeyed every 12 hours)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 4096-bit CA for Test PIV Cards v2

Validity: Not Before: Oct 20 14:00:02 2020 GMT, Not After: Oct 22 14:00:02 2020 GMT

Subject: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 4096-bit CA's OCSP Responder

Subject Public Key Info: rsaEncryption, 4096-bit modulus, e=65537

Extensions:

Authority Key Identifier:

0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Key Usage: critical

Digital Signature

Extended Key Usage:

OCSP Signing

OCSP No Check:

Certificate Policies:

id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning

Subject Key Identifier:

SHA-1 hash of subject public key

D.3.4 ECC P256 CA OCSP Responder Certificate

Serial Number: x (short lifetime certificate rekeyed every 12 hours)

Signature Algorithm: ecdsa-with-SHA256

Issuer: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test ECC P-256 CA for Test PIV Cards v2

Validity: Not Before: Oct 20 14:00:01 2020 GMT, Not After: Oct 22 14:00:01 2020 GMT

Subject: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test ECC P-256 CA's OCSP Responder

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Key Usage: critical

Digital Signature

Extended Key Usage:

OCSP Signing

OCSP No Check:

Certificate Policies:

id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning

Subject Key Identifier:

SHA-1 hash of subject public key

D.3.5 ECC P-384 CA OCSP Responder Certificate

Serial Number: x (short lifetime certificate rekeyed every 12 hours)

Signature Algorithm: ecdsa-with-SHA384

Issuer: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test ECC P-384 CA for Test PIV Cards v2

Validity: Not Before: Oct 20 14:00:01 2020 GMT, Not After: Oct 22 14:00:01 2020 GMT

Subject: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test ECC P-384 CA's OCSP Responder

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Key Usage: critical

Digital Signature

Extended Key Usage:

OCSP Signing

OCSP No Check:

Certificate Policies:

id_fpki_common_hardware
id_fpki_common_authentication
id_fpki_common_cardAuth
id_fpki_common_piv_contentSigning

Subject Key Identifier:

SHA-1 hash of subject public key

D.3.6 RSA 2048-bit PIV-I CA OCSP Responder Certificate

Serial Number: x (short lifetime certificate rekeyed every 12 hours)

Signature Algorithm: sha256WithRSAEncryption

Issuer: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test PIV-I RSA 2048-bit CA for Test PIV Cards v2

Validity: Not Before: Oct 20 14:00:01 2020 GMT, Not After: Oct 22 14:00:01 2020 GMT

Subject: C = US, O = Test Certificates 2020, OU = Test CA, CN = Test RSA 2048-bit CA's OCSP Responder

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

Key Usage: critical

Digital Signature

Extended Key Usage:

OCSP Signing

OCSP No Check:

Certificate Policies:

id_pivi_issuer_certpcy_hardware
id_pivi_issuer_certpcy_cardAuth
id_pivi_issuer_certpcy_contentSigning

Subject Key Identifier:

SHA-1 hash of subject public key

D.4 Test PIV Cards

D.4.1 Test PIV Card 1

D.4.1.1 Test PIV Card 1: PIV Authentication Certificate

Status: not revoked

Serial Number: 101 (0x65)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
31:2F:81:4F:88:21:D9:A7:67:01:36:6D:F9:1F:A1:1A:EC:B8:99:D4

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage:
TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:
id_fpki_common_authentication

id_piv_NACI:
FALSE

Subject Alternative Name:
UPN:32015465737401@upn.example.com
FASC-N:D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED (Agency Code=3201/System Code=0295/Credential Number=834563/CS=1/ICI=2/PI=6464979587/OC=1/OI=3201/POA=1)
URI:urn:uuid:26092f20-f792-4f7f-94b2-d0923cce6c7a

D.4.1.2 Test PIV Card 1: Card Authentication Certificate

Status: not revoked

Serial Number: 102 (0x66)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
0E:90:00:FF:FD:CD:23:8B:58:C9:36:02:E3:F8:CA:33:A2:4B:41:19

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED (Agency Code=3201/System Code=0295/Credential Number=834563/CS=1/ICI=2/PI=6464979587/ OC=1/OI=3201/POA=1)
URI:urn:uuid:26092f20-f792-4f7f-94b2-d0923cce6c7a

D.4.1.3 Test PIV Card 1: Digital Signature Certificate

Status: not revoked

Serial Number: 103 (0x67)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

5A:D9:0B:0F:7C:F8:71:32:80:CE:CB:E8:E0:4B:95:8D:C9:A5:DC:47

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder@mail.example.com

D.4.1.4 Test PIV Card 1: Key Management Certificate

Status: not revoked

Serial Number: 104 (0x68)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
7E:FA:BD:32:8D:AE:89:90:48:14:EB:CB:63:31:FC:E9:54:CE:02:E0

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder@mail.example.com

D.4.1.5 Test PIV Card 1: Retired Key Management Certificate A

Serial Number: 104 (0x68)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

D7:A9:62:92:7D:9A:9C:80:8E:74:B1:1F:76:44:69:D8:3E:34:99:6C

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder@mail.example.com

D.4.2 Test PIV Card 2

D.4.2.1 Test PIV Card 2: PIV Authentication Certificate

Status: not revoked

Serial Number: 201 (0xc9)

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: CN=Test RSA 3072-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Tëst Cardholder Jr. (affiliate), ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier: 9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Subject Key Identifier: 2C:C7:0E:68:99:47:54:0F:2E:EF:CF:E4:65:42:E2:2D:3B:20:78:9B

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA3072IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA3072IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies: id_fpki_common_authentication

id_piv_NACI: FALSE

Subject Alternative Name:

FASC-N:D6501858289D6C1C92ADE58360D8210842108421084210871E4 (Agency Code=3201/System Code=0295/Credential Number=034567/CS=0/ICI=0/PI=0000000000/OC=0/OI=0000/POA=0)

URI:urn:uuid:44be5385-2e86-434d-b45e-b3e09fcc0dca

D.4.2.2 Test PIV Card 2: Card Authentication Certificate

Status: not revoked

Serial Number: 202 (0xca)

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: CN=Test RSA 3072-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject:

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Subject Key Identifier:

8A:3E:1E:23:33:2E:DB:90:D8:0B:74:96:77:7F:6E:5F:90:C8:9C:AD

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA3072IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA3072IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage: critical, id_piv_cardAuth

Certificate Policies: id_fpki_common_cardAuth

id_piv_NACI: FALSE

Subject Alternative Name: critical

FASC-N:D6501858289D6C1C92ADE58360D8210842108421084210842087E4 (Agency Code=3201/System Code=0295/Credential Number=034567/CS=0/ICI=0/PI=0000000000/OC=0/OI=0000/POA=0)

URI:urn:uuid:44be5385-2e86-434d-b45e-b3e09fcc0dca

D.4.2.3 Test PIV Card 2: Digital Signature Certificate

Status: not revoked

Serial Number: 203 (0xcb)

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: CN=Test RSA 3072-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Tëst Cardholder Jr. (affiliate), ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Subject Key Identifier:

AE:DC:AD:59:57:AF:7C:E2:7A:5F:F5:22:06:31:85:CB:27:0F:21:94

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA3072IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA3072IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Extended Key Usage:

E-mail Protection, id-msft-document-signing

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder2@mail.example.com

D.4.2.4 Test PIV Card 2: Key Management Certificate

Status: not revoked

Serial Number: 204 (0xcc)

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: CN=Test RSA 3072-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Tëst Cardholder Jr. (affiliate), ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

9A:DC:09:A8:E7:3A:B2:F9:3B:76:48:D6:26:8C:AD:D6:99:5C:23:9C

Subject Key Identifier:

44:95:4D:DD:53:5C:5B:A3:46:00:AF:DB:76:E8:87:49:D6:4E:C6:D7

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA3072IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA3072IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20RSA%203072-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder2@mail.example.com

D.4.2.5 Test PIV Card 2: Retired Key Management Certificate A

Serial Number: 204 (0xcc)

Signature Algorithm: rsassaPss

Hash Algorithm: sha256
Mask Algorithm: mgf1 with sha256
Salt Length: 0x20
Trailer Field: 0xBC (default)

Issuer: CN=Test RSA 3072-bit CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder Jr. (affiliate), ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:6C:4D:F0:57:3A:E5:2D:89:5F:BD:12:24:3D:4B:B3:E4:55:D3:7D

Subject Key Identifier:

05:DC:19:F7:C0:5A:8C:F1:5E:19:12:24:EB:A0:CF:FC:F7:32:CF:AC

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA3072CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder2@mail.example.com

D.4.3 Test PIV Card 3

D.4.3.1 Test PIV Card 3: PIV Authentication Certificate

Status: not revoked

Serial Number: 301 (0x12d)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 4096-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185855E56DC8127945A16CDB906E7880C08286501843F5, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Subject Key Identifier:
8E:2A:F8:01:56:67:EF:11:FB:BC:7E:C6:17:38:31:9E:FB:EA:4C:6A

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA4096IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA4096IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage:
TLS Web Client Authentication, Microsoft Smartcard Login

Certificate Policies:
id_fpki_common_authentication

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D650185855E56DC8127945A16CDB906E7880C08286501843F5 (Agency Code=3201/System Code=8575/Credential Number=714932/CS=1/ICI=3/PI=7163720148/OC=1/OI=3201/POA=1)
URI:urn:uuid:45853470-a403-4844-ae15-c6495959fad5

D.4.3.2 Test PIV Card 3: Card Authentication Certificate

Status: not revoked

Serial Number: 302 (0x12e)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 4096-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185855E56DC8127945A16CDB906E7880C08286501843F5, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Subject Key Identifier:
B7:C2:30:0A:30:CC:B9:37:CD:86:22:40:E6:DF:E6:28:47:CC:0E:79

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA4096IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA4096IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D650185855E56DC8127945A16CDB906E7880C08286501843F5 (Agency Code=3201/System Code=8575/Credential Number=714932/CS=1/ICI=3/PI=7163720148/ OC=1/OI=3201/POA=1)
URI:urn:uuid:45853470-a403-4844-ae15-c6495959fad5

D.4.3.3 Test PIV Card 3: Digital Signature Certificate

Status: not revoked

Serial Number: 303 (0x12f)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 4096-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder III, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Subject Key Identifier:
F3:EE:37:35:D1:E2:B5:B3:BB:85:BD:26:66:05:AC:9B:49:61:02:D4

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA4096IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA4096IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection, id-msft-document-signing

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder3@mail.example.com

D.4.3.4 Test PIV Card 3: Key Management Certificate

Status: not revoked

Serial Number: 304 (0x130)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 4096-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder III, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
0D:8E:AC:1D:87:9F:77:08:EB:D5:EB:DB:30:B9:CB:1F:20:89:51:E4

Subject Key Identifier:
A0:B0:2B:99:94:1E:A4:4B:4F:2C:67:3D:15:AF:19:83:92:9B:35:26

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA4096IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA4096IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder3@mail.example.com

D.4.3.5 Test PIV Card 3: Retired Key Management Certificate A

Serial Number: 305 (0x131)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Nov 17 17:23:14 2006 GMT, Not After: Nov 17 17:23:14 2008 GMT

Subject: CN=Test Cardholder III, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

Authority Key Identifier:

15:40:EC:5B:D2:37:35:34:01:1E:3D:2E:04:C1:5F:5E:2F:55:02:F6

Subject Key Identifier:

20:68:6C:00:A0:59:DF:7D:E2:C1:67:AA:84:4B:81:59:73:20:45:68

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://p7c.example.com/PIVTest/CACertsIssuedToRSA1024CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder3@mail.example.com

D.4.3.6 Test PIV Card 3: Retired Key Management Certificate B

Serial Number: 306 (0x132)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2007 GMT, Not After: Apr 3 19:56:01 2009 GMT

Subject: CN=Test Cardholder III, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

62:EB:8F:8B:C1:29:7C:FD:C4:87:5A:1D:2B:89:D8:22:AB:F9:29:21

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder3@mail.example.com

D.4.3.7 Test PIV Card 3: Retired Key Management Certificate C

Serial Number: 307 (0x133)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Jul 26 20:12:48 2008 GMT, Not After: Jul 26 20:12:48 2028 GMT

Subject: CN=Test Cardholder III, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

96:30:C6:36:CF:08:F3:D0:B9:1D:A7:31:C6:FB:CA:93:7A:DC:C4:15

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder3@mail.example.com

D.4.3.8 Test PIV Card 3: Retired Key Management Certificate D

Serial Number: 304 (0x130)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder III, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

45:82:44:E4:6C:3A:84:11:01:F2:A7:1D:62:BB:61:7D:DC:49:5D:DD

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder3@mail.example.com

D.4.4 Test PIV Card 4

D.4.4.1 Test PIV Card 4: PIV Authentication Certificate

Status: not revoked

Serial Number: 401 (0x191)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder IV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

A1:26:A1:A5:5A:CA:C8:46:6B:C1:C6:59:03:21:97:18:2B:4E:95:57

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies: id_fpki_common_authentication

id_piv_NACI: FALSE

Subject Alternative Name:

UPN:32011152472674@upn.example.com

FASC-N:D650185B3CCE6D9C905325A1625A10AA09C4378486501843EB (Agency Code=3201/System Code=3733/Credential Number=334894/CS=1/ICI=4/PI=1152472674/OC=1/OI=3201/POA=1)

URI:urn:uuid:a4eb5a09-66c3-4f3e-83f3-b77e0ee96a25

D.4.4.2 Test PIV Card 4: Card Authentication Certificate

Status: not revoked

Serial Number: 402 (0x192)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185B3CCE6D9C905325A1625A10AA09C4378486501843EB, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

B3:0A:53:FF:D7:B7:37:EB:88:F2:4B:32:C8:F7:08:06:07:FE:37:45

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage: critical, id_piv_cardAuth

Certificate Policies: id_fpki_common_cardAuth

id_piv_NACI: FALSE

Subject Alternative Name:

FASC-N:D650185B3CCE6D9C905325A1625A10AA09C4378486501843EB (Agency Code=3201/System Code=3733/Credential Number=334894/CS=1/ICI=4/PI=1152472674/OC=1/OI=3201/POA=1)

URI:urn:uuid:a4eb5a09-66c3-4f3e-83f3-b77e0ee96a25

D.4.4.3 Test PIV Card 4: Digital Signature Certificate

Status: not revoked

Serial Number: 403 (0x193)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder IV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

53:06:8B:88:D3:AA:A5:00:C1:1C:C2:73:31:8F:CC:D8:15:EA:34:43

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Extended Key Usage:

E-mail Protection, id-msft-document-signing

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.4 Test PIV Card 4: Key Management Certificate

Status: not revoked

Serial Number: 404 (0x194)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder IV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

9A:70:25:7A:82:CB:15:97:43:AF:C5:B1:10:2D:29:3C:7C:FB:2B:33

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.5 Test PIV Card 4: Retired Key Management Certificate A

Serial Number: 405 (0x195)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2005 GMT, Not After: Apr 3 19:56:01 2008 GMT

Subject: CN=Test E. Cardholder IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

8F:E6:D5:CC:AE:19:62:12:60:E6:A7:35:CE:84:CF:3E:E4:67:7D:53

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.6 Test PIV Card 4: Retired Key Management Certificate B

Serial Number: 406 (0x196)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2006 GMT, Not After: May 19 19:56:01 2009 GMT

Subject: CN=Test E. Cardholder IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

0A:F3:C6:29:87:94:8F:92:71:21:27:33:F5:7E:9E:F3:90:25:A2:FA

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.7 Test PIV Card 4: Retired Key Management Certificate C

Serial Number: 407 (0x197)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Mar 2 11:17:23 2007 GMT, Not After: Mar 2 11:17:23 2010 GMT

Subject: CN=Test E. Cardholder IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

0E:EF:47:3C:22:05:EC:B8:23:81:96:7E:13:85:96:AA:05:DC:95:92

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.8 Test PIV Card 4: Retired Key Management Certificate D

Serial Number: 408 (0x198)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Sep 25 23:18:12 2008 GMT, Not After: Sep 25 23:18:12 2011 GMT

Subject: CN=Test E. Cardholder IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

3B:F2:A7:0F:0C:DA:32:BE:0E:C5:B4:73:5A:AF:A2:93:5C:4C:2C:4F

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.9 Test PIV Card 4: Retired Key Management Certificate E

Serial Number: 409 (0x199)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Mar 12 02:04:01 2009 GMT, Not After: Mar 12 02:04:01 2012 GMT

Subject: CN=Test E. Cardholder IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

4E:C4:BF:C7:44:3F:6B:09:B3:67:F7:73:75:AC:07:B3:9A:4E:87:17

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.10 Test PIV Card 4: Retired Key Management Certificate F

Serial Number: 404 (0x194)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test E. Cardholder IV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

95:1E:1F:CE:CB:FC:0B:96:31:CA:26:03:C7:D0:9E:3C:FF:B4:B7:49

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.11 Test PIV Card 4: Retired Key Management Certificate G

Serial Number: 405 (0x195)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2015 GMT, Not After: Aug 5 08:30:00 2018 GMT

Subject: CN=Test Cardholder IV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

A0:87:C4:EC:83:D6:CA:3E:B8:5A:19:C1:9F:C9:7A:D3:9E:26:8A:F2

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.12 Test PIV Card 4: Retired Key Management Certificate H

Serial Number: 406 (0x196)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2016 GMT, Not After: Aug 5 08:30:00 2019 GMT

Subject: CN=Test Cardholder IV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

0A:E3:72:E1:06:E6:21:DC:46:B0:4A:C3:03:7B:0F:03:2C:F5:58:7D

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.4.13 Test PIV Card 4: Retired Key Management Certificate I

Serial Number: 407 (0x197)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2017 GMT, Not After: Aug 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder IV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

1F:11:D8:34:6B:B6:64:E0:64:21:42:9F:C4:C7:9C:E3:B7:04:19:2C

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder4@mail.example.com

D.4.5 Test PIV Card 5

D.4.5.1 Test PIV Card 5: PIV Authentication Certificate

Status: not revoked

Serial Number: 501 (0x1f5)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder V, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

7C:88:DF:02:12:12:52:DB:8C:3C:74:6A:0F:38:8E:29:1E:48:84:E7

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies: id_fpki_common_authentication

id_piv_NACI: FALSE

Subject Alternative Name:

URI:urn:uuid:be694761-f813-46cb-9d3a-28a0142f98e6

FASC-N:D650185A13422C2267930D9162589080501E649C86501843FC (Agency Code=3201/System Code=1922/Credential Number=843790/CS=2/ICI=4/PI=4110207347/OC=1/OI=3201/POA=1)

D.4.5.2 Test PIV Card 5: Card Authentication Certificate

Status: not revoked

Serial Number: 502 (0x1f6)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185A13422C2267930D9162589080501E649C86501843FC, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

0E:B5:DF:14:34:73:D6:F4:B9:3D:28:C8:D4:DB:5B:6D:7A:4B:35:24

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage: critical, id_piv_cardAuth

Certificate Policies: id_fpki_common_cardAuth

id_piv_NACI: FALSE

Subject Alternative Name:

FASC-N:D650185A13422C2267930D9162589080501E649C86501843FC (Agency Code=3201/System Code=1922/Credential Number=843790/CS=2/ICI=4/PI=4110207347/OC=1/OI=3201/POA=1)

URI:urn:uuid:be694761-f813-46cb-9d3a-28a0142f98e6

D.4.5.3 Test PIV Card 5: Digital Signature Certificate

Status: not revoked

Serial Number: 503 (0x1f7)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder V, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

3B:E5:15:CC:A8:D1:4F:AE:4E:C4:3A:91:9D:7C:3E:08:A9:6E:A9:46

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Extended Key Usage:

E-mail Protection, id-msft-document-signing

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.4 Test PIV Card 5: Key Management Certificate

Status: not revoked

Serial Number: 504 (0x1f8)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder V, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

D7:A5:D8:72:41:A8:54:1C:98:E0:B2:2C:AA:C7:6A:AD:A0:0E:8A:3F

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.5 Test PIV Card 5: Retired Key Management Certificate A

Serial Number: 505 (0x1f9)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2005 GMT, Not After: Apr 3 19:56:01 2008 GMT

Subject: CN=Test E. Cardholder V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

59:1B:21:1F:A7:C0:B2:BC:70:35:6C:98:52:91:6F:4B:3E:B6:5F:73

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.6 Test PIV Card 5: Retired Key Management Certificate B

Serial Number: 506 (0x1fa)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2006 GMT, Not After: May 19 19:56:01 2009 GMT

Subject: CN=Test E. Cardholder V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

E8:CA:0D:AD:BE:7C:F4:FE:A7:9C:60:D5:A5:30:B8:0F:F2:7B:34:DA

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.7 Test PIV Card 5: Retired Key Management Certificate C

Serial Number: 507 (0x1fb)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Sep 25 23:18:12 2007 GMT, Not After: Sep 25 23:18:12 2010 GMT

Subject: CN=Test E. Cardholder V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

E5:4D:F3:FB:94:C1:99:5A:8A:77:C2:F2:D2:B0:01:40:64:39:94:17

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.8 Test PIV Card 5: Retired Key Management Certificate D

Serial Number: 508 (0x1fc)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Sep 25 23:18:12 2008 GMT, Not After: Sep 25 23:18:12 2011 GMT

Subject: CN=Test E. Cardholder V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

E7:B0:E5:6D:4D:93:AA:12:4C:3C:16:C1:9A:26:96:67:B3:51:B0:49

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.9 Test PIV Card 5: Retired Key Management Certificate E

Serial Number: 509 (0x1fd)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

Validity: Not Before: Sep 25 23:18:12 2009 GMT, Not After: Sep 25 23:18:12 2012 GMT

Subject: CN=Test E. Cardholder V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

81:01:01:B0:2D:45:E7:BF:51:C4:F9:28:81:0C:90:49:A3:88:E3:42

Subject Key Identifier:

08:83:02:8B:69:85:DB:70:58:B9:ED:6D:C7:E8:86:50:37:54:BE:22

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-384CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.5.10 Test PIV Card 5: Retired Key Management Certificate F

Serial Number: 504 (0x1f8)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards, ou=Test CA, o=Test Certificates 2010, c=US

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test E. Cardholder V, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

81:01:01:B0:2D:45:E7:BF:51:C4:F9:28:81:0C:90:49:A3:88:E3:42

Subject Key Identifier:

9E:08:18:11:30:D4:C0:F7:4C:A7:C1:14:86:7D:09:3D:13:3E:A1:58

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-384CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder5@mail.example.com

D.4.6 Test PIV Card 6

D.4.6.1 Test PIV Card 6: PIV Authentication Certificate

Status: not revoked

Serial Number: 601 (0x259)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D65018582214EC29D72125A1645899207990B49086501857E1, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

D6:3B:5A:EF:91:DC:14:5B:4A:83:EA:59:C8:9F:65:21:4B:8E:77:6F

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

TRUE

Subject Alternative Name:

FASC-N:D65018582214EC29D72125A1645899207990B49086501857E1 (Agency Code=3201/System Code=0889/Credential Number=895304/CS=1/ICI=2/PI=4340730641/OC=1/OI=3201/POA=5)

URI:urn:uuid:0a40b578-723f-42c8-9923-09ecd0163d6a

D.4.6.2 Test PIV Card 6: Card Authentication Certificate

Status: not revoked

Serial Number: 602 (0x25a)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D65018582214EC29D72125A1645899207990B49086501857E1, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
31:90:FD:6A:1A:B0:E0:EB:79:B0:7B:96:0B:54:1D:71:66:D7:D9:22

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
TRUE

Subject Alternative Name:
FASC-N:D65018582214EC29D72125A1645899207990B49086501857E1 (Agency Code=3201/System Code=0889/Credential Number=895304/CS=1/ICI=2/PI=4340730641/OC=1/OI=3201/POA=5)
URI:urn:uuid:0a40b578-723f-42c8-9923-09ecd0163d6a

D.4.7 Test PIV Card 7

D.4.7.1 Test PIV Card 7: PIV Authentication Certificate

Status: not revoked

Serial Number: 701 (0x2bd)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

AB:27:1D:87:F6:FD:1E:7F:16:A8:AD:9D:1D:9E:AC:BC:83:56:34:66

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

FALSE

Subject Alternative Name:

FASC-N:D650185A1C84EC10850D6DA16E5B958121C0B61C86501843E8 (Agency Code=3201/System Code=1719/Credential Number=000266/CS=1/ICI=7/PI=7514170617/ OC=1/OI=3201/POA=1)

UPN:testcardholder7@upn.example.net

URI:urn:uuid:9a4b12d1-d28c-498c-8182-37875ac7a0c4

D.4.7.2 Test PIV Card 7: Card Authentication Certificate

Status: not revoked

Serial Number: 702 (0x2be)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185A1C84EC10850D6DA16E5B958121C0B61C86501843E8, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
31:E9:28:D4:19:1C:F5:01:FD:53:40:68:34:92:0C:BD:C6:32:4D:A3

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D650185A1C84EC10850D6DA16E5B958121C0B61C86501843E8 (Agency Code=3201/System Code=1719/Credential Number=000266/CS=1/ICI=7/PI=7514170617/ OC=1/OI=3201/POA=1)
URI:urn:uuid:9a4b12d1-d28c-498c-8182-37875ac7a0c4

D.4.7.3 Test PIV Card 7: Digital Signature Certificate

Status: not revoked

Serial Number: 703 (0x2bf)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

93:AC:73:83:0C:95:85:DA:E4:52:C4:3C:C0:BA:4C:CB:E1:B5:56:1A

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.7.4 Test PIV Card 7: Key Management Certificate

Status: not revoked

Serial Number: 704 (0x2c0)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
32:73:F6:A8:84:34:8E:42:2A:68:8C:D1:53:10:0D:E0:00:6D:A7:30

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder7@mail.example.com

D.4.7.5 Test PIV Card 7: Retired Key Management Certificate A

Serial Number: 705 (0x2c1)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2005 GMT, Not After: May 19 19:56:01 2008 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

EC:98:FB:0B:60:5B:6F:5A:DE:E6:65:43:D7:9E:75:22:3A:F1:F0:99

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.7.6 Test PIV Card 7: Retired Key Management Certificate B

Serial Number: 706 (0x2c2)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2006 GMT, Not After: May 19 19:56:01 2009 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

A4:06:84:38:40:86:96:55:47:F3:F6:47:67:26:61:CF:B5:80:E1:1F

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.7.7 Test PIV Card 7: Retired Key Management Certificate C

Serial Number: 707 (0x2c3)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2007 GMT, Not After: May 19 19:56:01 2010 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

CB:69:88:67:71:98:F5:20:C8:F7:C2:9D:28:25:9F:EC:6F:D0:11:04

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.7.8 Test PIV Card 7: Retired Key Management Certificate D

Serial Number: 708 (0x2c4)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2008 GMT, Not After: May 19 19:56:01 2011 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

2E:01:8F:FA:B5:8E:B3:49:F5:6E:8F:FA:56:CC:E7:EF:34:F9:C2:85

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.7.9 Test PIV Card 7: Retired Key Management Certificate E

Serial Number: 709 (0x2c5)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2009 GMT, Not After: May 19 19:56:01 2012 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

92:27:4F:FC:D1:ED:D1:AB:BD:40:94:81:11:0C:BE:4E:86:28:23:1B

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.7.10 Test PIV Card 7: Retired Key Management Certificate F

Serial Number: 704 (0x2c0)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder VII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

43:16:0B:80:C2:A5:D8:D4:39:B3:A1:3C:6D:F6:A9:2D:89:6C:11:7D

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder7@mail.example.com

D.4.8 Test PIV Card 8

D.4.8.1 Test PIV Card 8: PIV Authentication Certificate

Status: not revoked

Serial Number: 3f:e6:5e:2f:09:eb:9c:7d:70:40:85:d0:1d:f0:04:3e:e8:af:74:00

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

68:49:74:B8:90:06:BE:2C:7B:E2:90:D4:EF:62:89:23:93:B5:A9:15

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

SSH Client, TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

TRUE

Subject Alternative Name:

FASC-N:D6501859ADA92C1E5602E5A169DB9545450692B086501843ED (Agency Code=3201/System Code=6654/Credential Number=075187/CS=1/ICI=9/PI=7525816451/ OC=1/OI=3201/POA=1)

UPN:32017525816451@upn.example.com

URI:urn:uuid:12b9c2c3-8e0e-4cbe-a0d1-fc906174bb94

D.4.8.2 Test PIV Card 8: Card Authentication Certificate

Status: not revoked

Serial Number: 51:b4:2f:0a:77:43:0e:56:54:22:64:a6:2a:88:7a:84:d4:89:a9:c6

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D6501859ADA92C1E5602E5A169DB9545450692B086501843ED, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
A1:D8:65:4C:DF:CF:CF:17:3F:CC:95:92:5E:AE:A3:18:C9:B2:A1:04

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
TRUE

Subject Alternative Name:
FASC-N:D6501859ADA92C1E5602E5A169DB9545450692B086501843ED (Agency Code=3201/System Code=6654/Credential Number=075187/CS=1/ICI=9/PI=7525816451/ OC=1/OI=3201/POA=1)
URI:urn:uuid:12b9c2c3-8e0e-4cbe-a0d1-fc906174bb94

D.4.8.3 Test PIV Card 8: Digital Signature Certificate

Status: not revoked

Serial Number: 40:78:f2:09:34:36:dc:9c:a9:3c:77:b1:d9:7b:90:a2:90:ec:c3:af

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
F4:58:29:62:B0:92:53:93:86:67:02:E3:E6:08:88:9C:51:B8:94:E1

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection, id-msft-document-signing

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder8@mail.example.com

D.4.8.4 Test PIV Card 8: Key Management Certificate

Status: not revoked

Serial Number: 07:59:92:a5:31:a8:b0:50:e2:c5:af:82:38:60:8c:6b:49:fe:a8:81

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
31:1A:54:58:D6:54:57:ED:C0:D7:B7:82:64:48:75:CC:F1:C1:62:B0

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder8@mail.example.com

D.4.8.5 Test PIV Card 8: Retired Key Management Certificate A

Serial Number: 805 (0x325)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: May 19 19:56:01 2005 GMT, Not After: May 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

1A:F5:94:CB:B1:17:DE:8F:F6:78:8D:A7:4B:D4:7D:9B:E1:95:E7:B5

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.6 Test PIV Card 8: Retired Key Management Certificate B

Serial Number: 806 (0x326)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Jun 19 19:56:01 2005 GMT, Not After: Jun 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

D7:EE:40:B2:C8:9A:7C:8D:E0:3F:BF:F9:E5:E5:73:81:9B:22:9B:24

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.7 Test PIV Card 8: Retired Key Management Certificate C

Serial Number: 807 (0x327)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Jul 19 19:56:01 2005 GMT, Not After: Jul 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

CB:EB:3C:78:0C:C7:B0:55:42:B0:76:FE:53:A1:A0:11:56:94:F2:04

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.8 Test PIV Card 8: Retired Key Management Certificate D

Serial Number: 808 (0x328)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Aug 19 19:56:01 2005 GMT, Not After: Aug 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

93:F4:34:CA:38:29:92:61:01:83:06:9A:FE:20:1D:30:29:DF:9C:A2

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.9 Test PIV Card 8: Retired Key Management Certificate E

Serial Number: 809 (0x329)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Sep 19 19:56:01 2005 GMT, Not After: Sep 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

DC:C4:44:34:96:37:34:B1:12:95:57:71:C4:6F:5A:5C:88:B0:85:BC

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.10 Test PIV Card 8: Retired Key Management Certificate F

Serial Number: 810 (0x32a)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Oct 19 19:56:01 2005 GMT, Not After: Oct 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

39:5F:01:6E:DF:F4:DE:E4:2F:B6:4A:B5:61:09:DA:54:54:8B:DE:75

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.11 Test PIV Card 8: Retired Key Management Certificate G

Serial Number: 811 (0x32b)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Nov 19 19:56:01 2005 GMT, Not After: Nov 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

A3:99:63:DC:60:BC:DC:89:A8:FA:A7:14:72:25:FD:6B:08:36:8B:02

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.12 Test PIV Card 8: Retired Key Management Certificate H

Serial Number: 812 (0x32c)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Dec 19 19:56:01 2005 GMT, Not After: Dec 19 19:56:01 2008 GMT

Subject: CN=Example Cardholder, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

0A:BA:E1:A3:E3:80:11:39:AA:E5:B6:CC:70:04:AA:06:1B:D9:9A:D0

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:example.cardholder@mail.example.com

D.4.8.13 Test PIV Card 8: Retired Key Management Certificate I

Serial Number: 813 (0x32d)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Jul 26 20:12:48 2008 GMT, Not After: Jul 26 20:12:48 2011 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

6C:CA:C2:E1:08:A8:4D:D9:A9:34:D8:C1:FF:1C:70:0B:60:7A:73:24

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.14 Test PIV Card 8: Retired Key Management Certificate J

Serial Number: 814 (0x32e)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Jul 26 20:12:48 2009 GMT, Not After: Jul 26 20:12:48 2012 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

60:25:DD:C6:9A:FB:5A:50:E1:86:A4:08:FE:CE:E9:44:21:D8:EB:F1

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.15 Test PIV Card 8: Retired Key Management Certificate K

Serial Number: 58:22:b6:5e:83:60:b2:3d:89:3d:45:78:37:21:dc

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

1D:6B:0A:88:08:1A:D7:F1:16:AB:D9:FE:58:87:5D:0E:F6:FE:F2:58

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.16 Test PIV Card 8: Retired Key Management Certificate L

Serial Number: 812 (0x32c)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Feb 6 08:30:00 2011 GMT, Not After: Feb 6 08:30:00 2014 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
46:77:ED:B7:F9:4A:3D:28:53:F3:4C:32:53:F1:9B:04:6A:3F:56:10

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder8@mail.example.com

D.4.8.17 Test PIV Card 8: Retired Key Management Certificate M

Serial Number: 813 (0x32d)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 6 08:30:00 2011 GMT, Not After: Aug 6 08:30:00 2014 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

5F:EA:ED:0E:D9:C1:25:FE:07:74:65:B1:4E:85:6B:A0:3F:21:1A:DA

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.18 Test PIV Card 8: Retired Key Management Certificate N

Serial Number: 814 (0x32e)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Mar 6 08:30:00 2012 GMT, Not After: Mar 6 08:30:00 2015 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
E0:4F:82:0E:94:D7:22:C5:F8:98:84:BB:D8:92:65:17:AA:8C:2C:E1

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder8@mail.example.com

D.4.8.19 Test PIV Card 8: Retired Key Management Certificate O

Serial Number: 815 (0x32f)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 6 08:30:00 2012 GMT, Not After: Aug 6 08:30:00 2015 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

89:38:28:04:F4:0A:1A:B7:41:60:B3:23:BE:F4:33:A4:4C:58:01:97

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.20 Test PIV Card 8: Retired Key Management Certificate P

Serial Number: 816 (0x330)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Mar 6 08:30:00 2013 GMT, Not After: Mar 6 08:30:00 2016 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

8C:F7:38:4C:5D:F4:A6:6D:7B:83:5C:58:15:6E:8B:81:24:50:CB:3A

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.21 Test PIV Card 8: Retired Key Management Certificate Q

Serial Number: 817 (0x331)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 6 08:30:00 2013 GMT, Not After: Aug 6 08:30:00 2016 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

50:76:05:B3:28:AE:49:ED:0D:8A:90:64:4F:EA:15:9E:1F:6B:A9:26

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.22 Test PIV Card 8: Retired Key Management Certificate R

Serial Number: 818 (0x332)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Apr 6 08:30:00 2014 GMT, Not After: Apr 6 08:30:00 2017 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

BA:6A:2F:BD:B0:6F:4B:EA:37:46:96:23:93:B2:3B:0E:A2:9A:D6:4F

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.23 Test PIV Card 8: Retired Key Management Certificate S

Serial Number: 819 (0x333)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 6 08:30:00 2014 GMT, Not After: Aug 6 08:30:00 2017 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

86:1B:87:55:DF:95:D0:3A:6B:C2:47:4A:CC:37:F3:3D:7F:7B:55:F8

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.8.24 Test PIV Card 8: Retired Key Management Certificate T

Serial Number: 820 (0x334)

Signature Algorithm: ecdsa-with-SHA384

Issuer: CN=Test ECC P-384 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 6 08:30:00 2016 GMT, Not After: Aug 6 08:30:00 2019 GMT

Subject: CN=Test Cardholder VIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-384

Extensions:

Authority Key Identifier:

A1:A9:F2:66:2C:F8:29:F4:13:0C:7B:ED:5B:64:68:94:3D:F3:F1:BC

Subject Key Identifier:

AE:33:31:28:C6:A2:74:88:E2:86:6B:E2:31:AB:D5:10:ED:B7:C7:07

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP384IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP384IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-384%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder8@mail.example.com

D.4.9 Test PIV Card 9

D.4.9.1 Test PIV Card 9: PIV Authentication Certificate

Status: not revoked

Serial Number: 901 (0x385)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Apr 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder IX (affiliate), ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

B1:24:99:0B:71:F7:A7:62:73:53:D0:AE:4E:22:F0:4A:19:5C:7F:42

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

TRUE

Subject Alternative Name:

UPN:32012243747282@upn.example.com

FASC-N:D650185AA4412D084E750DA164590826784E204886501857FC (Agency Code=3201/System Code=5424/Credential Number=119950/CS=1/ICI=2/PI=2243747282/OC=1/OI=3201/POA=5)

URI:urn:uuid:6a7c77e2-933d-4e40-84b6-6c903ae8d220

D.4.9.2 Test PIV Card 9: Card Authentication Certificate

Status: not revoked

Serial Number: 902 (0x386)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Apr 5 08:30:00 2020 GMT

Subject: serialNumber=D650185AA4412D084E750DA164590826784E204886501857FC, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
13:B1:66:7B:CE:D7:9A:CD:4C:BB:B6:3D:BB:1B:56:17:23:69:7E:73

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
TRUE

Subject Alternative Name:
FASC-N:D650185AA4412D084E750DA164590826784E204886501857FC (Agency Code=3201/System Code=5424/Credential Number=119950/CS=1/ICI=2/PI=2243747282/ OC=1/OI=3201/POA=5)
URI:urn:uuid:6a7c77e2-933d-4e40-84b6-6c903ae8d220

D.4.9.3 Test PIV Card 9: Digital Signature Certificate

Status: not revoked

Serial Number: 903 (0x387)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Apr 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder IX (affiliate), ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
E4:DB:74:65:A7:9D:98:F1:ED:92:41:A6:BA:29:5E:75:C8:71:89:62

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder9@mail.example.com

D.4.9.4 Test PIV Card 9: Key Management Certificate

Status: not revoked

Serial Number: 904 (0x388)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Apr 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder IX (affiliate), ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
6D:48:B0:56:68:19:B2:1E:B2:3C:B9:62:23:02:E8:0F:E8:FC:A3:45

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder9@mail.example.com

D.4.9.5 Test PIV Card 9: Retired Key Management Certificate A

Serial Number: 904 (0x388)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Mar 1 08:30:00 2011 GMT

Subject: CN=Test Cardholder IX (affiliate), ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

6E:21:69:E9:E7:35:04:A9:DD:71:E5:94:A9:FE:02:84:B5:08:7C:E6

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder9@mail.example.com

D.4.10 Test PIV Card 10

D.4.10.1 Test PIV Card 10: PIV Authentication Certificate

Status: revoked

Serial Number: 1001 (0x3e9)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

90:CA:FF:5F:36:AC:85:20:F1:11:7F:BF:6E:5B:0A:3E:76:3B:13:2F

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

FALSE

Subject Alternative Name:

UPN:32019545326551@upn.example.com

FASC-N:D650185A0D412D5AB4999DA1625A75257286D6B086501843EE (Agency Code=3201/System Code=1624/Credential Number=556439/CS=1/ICI=4/PI=9545326551/ OC=1/OI=3201/POA=1)

URI:urn:uuid:0375b685-f108-4df7-8dec-3a11ec525c6f

D.4.10.2 Test PIV Card 10: Card Authentication Certificate

Status: revoked

Serial Number: 1002 (0x3ea)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185A0D412D5AB4999DA1625A75257286D6B086501843EE, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

EF:F5:C0:76:EE:12:78:3A:B0:3E:57:09:0E:C2:37:94:E4:A1:21:9A

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_piv_cardAuth

Certificate Policies:

id_fpki_common_cardAuth

id_piv_NACI:

FALSE

Subject Alternative Name:

FASC-N:D650185A0D412D5AB4999DA1625A75257286D6B086501843EE (Agency Code=3201/System Code=1624/Credential Number=556439/CS=1/ICI=4/PI=9545326551/ OC=1/OI=3201/POA=1)

URI:urn:uuid:0375b685-f108-4df7-8dec-3a11ec525c6f

D.4.10.3 Test PIV Card 10: Digital Signature Certificate

Status: revoked

Serial Number: 1003 (0x3eb)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
D6:08:A8:BF:91:4E:D4:84:30:E5:75:BB:DC:CC:17:6B:B6:17:7B:FD

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder10@mail.example.com

D.4.10.4 Test PIV Card 10: Key Management Certificate

Status: revoked

Serial Number: 1004 (0x3ec)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
16:64:C7:6E:EF:AD:3C:01:0E:8F:AD:B8:0F:20:61:B4:27:AF:30:55

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder10@mail.example.com

D.4.10.5 Test PIV Card 10: Retired Key Management Certificate A

Serial Number: 1005 (0x3ed)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2005 GMT, Not After: Apr 3 19:56:01 2008 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

6B:FA:9B:22:0B:04:93:BF:15:AA:70:78:CD:80:A1:99:E8:8D:3F:B8

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder10@mail.example.com

D.4.10.6 Test PIV Card 10: Retired Key Management Certificate B

Serial Number: 1006 (0x3ee)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2006 GMT, Not After: Apr 3 19:56:01 2009 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

BC:FA:F3:B4:45:EB:4B:35:1E:23:29:F0:48:B2:DF:79:7C:B6:F1:B5

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder10@mail.example.com

D.4.10.7 Test PIV Card 10: Retired Key Management Certificate C

Serial Number: 1007 (0x3ef)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2007 GMT, Not After: Apr 3 19:56:01 2010 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

31:6C:73:A9:DD:78:71:B5:46:01:AF:01:67:C0:90:AB:3F:CD:17:D9

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder10@mail.example.com

D.4.10.8 Test PIV Card 10: Retired Key Management Certificate D

Serial Number: 1008 (0x3f0)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2008 GMT, Not After: Apr 3 19:56:01 2011 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

9F:9B:80:28:31:45:06:5D:D4:71:82:67:9D:C5:CA:B5:FF:CF:C6:DB

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder10@mail.example.com

D.4.10.9 Test PIV Card 10: Retired Key Management Certificate E

Serial Number: 1009 (0x3f1)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2009 GMT, Not After: Apr 3 19:56:01 2012 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

B5:6B:BD:9C:4D:8F:EE:C6:CA:71:BC:A5:27:A5:59:08:D9:BE:D2:7F

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder10@mail.example.com

D.4.10.10 Test PIV Card 10: Retired Key Management Certificate F

Serial Number: 1004 (0x3ec)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder X, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

81:9E:09:7D:0D:51:D6:6C:A4:B6:77:52:8B:25:38:B4:E9:CF:92:21

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder10@mail.example.com

D.4.11 Test PIV Card 11

D.4.11.1 Test PIV Card 11: PIV Authentication Certificate

Status: not revoked, but signature is invalid

Serial Number: 101 (0x65)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

31:2F:81:4F:88:21:D9:A7:67:01:36:6D:F9:1F:A1:1A:EC:B8:99:D4

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

FALSE

Subject Alternative Name:

UPN:32015465737401@upn.example.com

FASC-N:D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED (Agency Code=3201/System Code=0295/Credential Number=834563/CS=1/ICI=2/PI=6464979587/OC=1/OI=3201/POA=1)

URI:urn:uuid:26092f20-f792-4f7f-94b2-d0923cce6c7a

D.4.11.2 Test PIV Card 11: Card Authentication Certificate

Status: not revoked, but signature is invalid

Serial Number: 102 (0x66)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

0E:90:00:FF:FD:CD:23:8B:58:C9:36:02:E3:F8:CA:33:A2:4B:41:19

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_piv_cardAuth

Certificate Policies:

id_fpki_common_cardAuth

id_piv_NACI:

FALSE

Subject Alternative Name:

FASC-N:D6501858289D6C2C92ADCDA16459A46927C9D45C86501843ED (Agency Code=3201/System Code=0295/Credential Number=834563/CS=1/ICI=2/PI=6464979587/ OC=1/OI=3201/POA=1)

URI:urn:uuid:26092f20-f792-4f7f-94b2-d0923cce6c7a

D.4.11.3 Test PIV Card 11: Digital Signature Certificate

Status: not revoked, but signature is invalid

Serial Number: 103 (0x67)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
5A:D9:0B:0F:7C:F8:71:32:80:CE:CB:E8:E0:4B:95:8D:C9:A5:DC:47

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder@mail.example.com

D.4.11.4 Test PIV Card 11: Key Management Certificate

Status: not revoked, but signature is invalid

Serial Number: 104 (0x68)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
7E:FA:BD:32:8D:AE:89:90:48:14:EB:CB:63:31:FC:E9:54:CE:02:E0

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder@mail.example.com

D.4.12 Test PIV Card 12

D.4.12.1 Test PIV Card 12: PIV Authentication Certificate

Status: not revoked

Serial Number: 1201 (0x4b1)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

B7:2D:DD:AB:DE:64:B3:A1:3C:CB:D8:1B:16:F9:D7:FB:C4:48:24:F8

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

FALSE

Subject Alternative Name:

UPN:32014001354205@upn.example.com

FASC-N:D650185AB06F2D08110185A16458810C3352203586501843E2 (Agency Code=3201/System Code=5167/Credential Number=114201/CS=1/ICI=2/PI=4001354205/OC=1/OI=3201/POA=1)

URI:urn:uuid:1a559799-3079-4058-aedb-ec37a05473d9

D.4.12.2 Test PIV Card 12: Card Authentication Certificate

Status: not revoked

Serial Number: 1202 (0x4b2)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D650185AB06F2D08110185A16458810C3352203586501843E2, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
1B:BD:EA:0B:15:08:AA:3C:C0:27:52:06:38:0C:90:02:05:17:88:54

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D650185AB06F2D08110185A16458810C3352203586501843E2 (Agency Code=3201/System Code=5167/Credential Number=114201/CS=1/ICI=2/PI=4001354205/ OC=1/OI=3201/POA=1)
URI:urn:uuid:1a559799-3079-4058-aedb-ec37a05473d9

D.4.12.3 Test PIV Card 12: Digital Signature Certificate

Status: not revoked

Serial Number: 1203 (0x4b3)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
B6:E9:AC:FD:01:03:32:22:B6:8E:98:6F:E4:C3:BB:7D:E4:81:AC:27

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder12@mail.example.com

D.4.12.4 Test PIV Card 12: Key Management Certificate

Status: not revoked

Serial Number: 1204 (0x4b4)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
E9:92:A7:90:09:4B:A4:7F:D6:90:B4:2B:D3:A8:E8:6B:1F:EC:E6:F5

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder12@mail.example.com

D.4.12.5 Test PIV Card 12: Retired Key Management Certificate A

Serial Number: 1204 (0x4b4)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder XII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

F1:2F:B7:4D:C9:48:A8:29:86:00:1C:6D:76:3D:2C:51:A8:82:6F:3A

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder12@mail.example.com

D.4.13 Test PIV Card 13

D.4.13.1 Test PIV Card 13: PIV Authentication Certificate

Status: not revoked

Serial Number: 1301 (0x515)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2017 GMT, Not After: Aug 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

FB:02:13:20:05:66:A8:51:24:E1:4A:D8:34:1E:F5:C3:EF:34:20:0F

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

FALSE

Subject Alternative Name:

UPN:32018949244215@upn.example.com

FASC-N:D6501859019B6D0E708D6DA164585324D042221586501843EB (Agency Code=3201/System Code=2096/Credential Number=177466/CS=1/ICI=2/PI=8949244215/OC=1/OI=3201/POA=1)

URI:urn:uuid:af6a1130-2635-43ac-9c89-175e062b1343

D.4.13.2 Test PIV Card 13: Card Authentication Certificate

Status: not revoked

Serial Number: 1302 (0x516)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2017 GMT, Not After: Aug 5 08:30:00 2020 GMT

Subject: serialNumber=D6501859019B6D0E708D6DA164585324D042221586501843EB, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
9D:ED:49:A9:EA:63:7B:69:46:D3:A5:CB:EF:E0:28:24:E4:0E:62:AF

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D6501859019B6D0E708D6DA164585324D042221586501843EB (Agency Code=3201/System Code=2096/Credential Number=177466/CS=1/ICI=2/PI=8949244215/OC=1/OI=3201/POA=1)
URI:urn:uuid:af6a1130-2635-43ac-9c89-175e062b1343

D.4.13.3 Test PIV Card 13: Digital Signature Certificate

Status: not revoked

Serial Number: 1303 (0x517)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2017 GMT, Not After: Aug 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
F3:2A:8D:FB:C9:44:4C:83:5A:20:E9:32:83:5E:AC:61:EB:6A:62:99

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder13@mail.example.com

D.4.13.4 Test PIV Card 13: Key Management Certificate

Status: not revoked

Serial Number: 1304 (0x518)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2017 GMT, Not After: Aug 5 08:30:00 2020 GMT

Subject: CN=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
0F:08:22:6E:D6:41:97:86:56:56:E3:3B:7D:E7:46:7F:AD:4A:49:2E

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder13@mail.example.com

D.4.13.5 Test PIV Card 13: Retired Key Management Certificate A

Serial Number: 1304 (0x518)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Mar 1 08:30:00 2008 GMT, Not After: Mar 1 08:30:00 2011 GMT

Subject: CN=Test Cardholder XIII, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

F3:70:CF:EA:1C:6C:AC:EC:B5:56:D9:B4:FC:32:DA:B3:34:9D:B6:21

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA **Issuer**s - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder13@mail.example.com

D.4.14 Test PIV Card 14

D.4.14.1 Test PIV Card 14: PIV Authentication Certificate

Status: not revoked

Serial Number: 1401 (0x579)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:

E5:EC:D4:3D:D8:02:EE:00:6D:CF:2A:AB:41:8D:23:7F:71:3F:FC:0A

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_fpki_common_authentication

id_piv_NACI:

FALSE

Subject Alternative Name:

UPN:32016091935084@upn.example.com

FASC-N:D6501858999CED9992150DA166D9A19C279A844486501843EE (Agency Code=3201/System Code=4399/Credential Number=394150/CS=1/ICI=6/PI=6091935084/OC=1/OI=3201/POA=1)

URI:urn:uuid:71417603-ef9b-4651-812a-d023c8f8d592

D.4.14.2 Test PIV Card 14: Card Authentication Certificate

Status: not revoked

Serial Number: 1402 (0x57a)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D6501858999CED9992150DA166D9A19C279A844486501843EE, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
01:B3:46:79:4F:CF:13:AC:F6:84:FB:8D:B1:94:5F:30:38:C0:18:76

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature

Extended Key Usage: critical
id_piv_cardAuth

Certificate Policies:
id_fpki_common_cardAuth

id_piv_NACI:
FALSE

Subject Alternative Name:
FASC-N:D6501858999CED9992150DA166D9A19C279A844486501843EE (Agency Code=3201/System Code=4399/Credential Number=394150/CS=1/ICI=6/PI=6091935084/OC=1/OI=3201/POA=1)
URI:urn:uuid:71417603-ef9b-4651-812a-d023c8f8d592

D.4.14.3 Test PIV Card 14: Digital Signature Certificate

Status: not revoked

Serial Number: 1403 (0x57b)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
EB:AE:AF:A1:CB:7D:B5:4A:4B:9E:FB:0E:83:A3:B1:07:06:9A:22:63

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Digital Signature, Non-Repudiation

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder14@mail.example.com

D.4.14.4 Test PIV Card 14: Key Management Certificate

Status: not revoked

Serial Number: 1404 (0x57c)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
38:F1:24:AB:3B:ED:E9:1D:03:3E:0F:2A:C2:81:43:12:E8:0F:30:37

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder14@mail.example.com

D.4.14.5 Test PIV Card 14: Retired Key Management Certificate A

Serial Number: 1405 (0x57d)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2005 GMT, Not After: Apr 3 19:56:01 2008 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

1C:A8:DB:82:5D:5B:AD:35:A4:BE:E4:31:7B:DA:4E:A9:F7:F6:CC:DC

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder14@mail.example.com

D.4.14.6 Test PIV Card 14: Retired Key Management Certificate B

Serial Number: 1406 (0x57e)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2006 GMT, Not After: Apr 3 19:56:01 2009 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

E1:00:EF:82:B2:71:7C:6C:7D:BA:C9:95:25:C7:F4:6A:8A:38:F4:15

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder14@mail.example.com

D.4.14.7 Test PIV Card 14: Retired Key Management Certificate C

Serial Number: 1407 (0x57f)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2007 GMT, Not After: Apr 3 19:56:01 2010 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

D5:05:A4:6B:8F:9D:31:2A:10:76:10:BC:26:AC:CF:04:3B:29:3A:6F

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder14@mail.example.com

D.4.14.8 Test PIV Card 14: Retired Key Management Certificate D

Serial Number: 1408 (0x580)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2008 GMT, Not After: Apr 3 19:56:01 2011 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

21:67:92:98:E1:88:B1:B2:87:7E:C3:3B:9D:4A:C0:5F:08:2D:3E:86

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder14@mail.example.com

D.4.14.9 Test PIV Card 14: Retired Key Management Certificate E

Serial Number: 1409 (0x581)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2009 GMT, Not After: Apr 3 19:56:01 2012 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

2F:E6:A8:F1:68:F6:0D:EF:D5:1E:72:B5:A8:13:F7:61:64:73:E5:77

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder14@mail.example.com

D.4.14.10 Test PIV Card 14: Retired Key Management Certificate F

Serial Number: 1404 (0x57c)

Signature Algorithm: sha256WithRSAEncryption

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

8F:BE:8E:48:44:B4:DF:FA:B2:90:91:74:CD:03:57:C7:FF:E8:BD:0C

Subject Key Identifier:

8D:CA:E1:10:35:50:E4:73:F8:AB:CB:8C:69:B1:14:0A:D4:BD:81:C3

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToRSA2048CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder14@mail.example.com

D.4.14.11 Test PIV Card 14: Retired Key Management Certificate G

Serial Number: 1405 (0x57d)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2014 GMT, Not After: Aug 5 08:30:00 2017 GMT

Subject: CN=Test Cardholder XIV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:
A5:E9:44:0B:AA:5C:29:EC:B2:DF:5F:90:74:DC:A5:6F:58:65:54:35

Subject Key Identifier:
D1:9C:B7:6A:11:59:57:56:D5:F0:E2:C4:4C:D1:90:66:26:C9:3D:41

CRL Distribution Points:
http://smime2.nist.gov/PIVTest2/RSA2048IssuingCA.crl

Authority Information Access:
CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048IssuingCA.p7c
OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical
Key Encipherment

Extended Key Usage:
E-mail Protection

Certificate Policies:
id_fpki_common_hardware

Subject Alternative Name:
email:test.cardholder14@mail.example.com

D.4.15 Test PIV Card 15

D.4.15.1 Test PIV Card 15: PIV Authentication Certificate

Status: revoked

Serial Number: 1501 (0x5dd)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

B7:83:03:6B:4D:16:22:22:15:60:2B:BE:80:36:6B:BA:7B:48:28:BB

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies: id_fpki_common_authentication

id_piv_NACI: FALSE

Subject Alternative Name:

UPN:32017241649364@upn.example.com

FASC-N:D65018591C422CD9E51CE5A16ADB88241A49E5A486501843E7 (Agency Code=3201/System Code=2722/Credential Number=693277/CS=1/ICI=5/PI=7241649364/OC=1/OI=3201/POA=1)

URI:urn:uuid:6c4ecd74-88c4-4828-9521-4902c8b4687c

D.4.15.2 Test PIV Card 15: Card Authentication Certificate

Status: revoked

Serial Number: 1502 (0x5de)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=D65018591C422CD9E51CE5A16ADB88241A49E5A486501843E7, OU=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

D2:F8:3C:21:36:E6:FA:58:07:85:C0:CB:96:04:EA:DA:64:13:8F:C4

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical, Digital Signature

Extended Key Usage: critical, id_piv_cardAuth

Certificate Policies: id_fpki_common_cardAuth

id_piv_NACI: FALSE

Subject Alternative Name:

FASC-N:D65018591C422CD9E51CE5A16ADB88241A49E5A486501843E7 (Agency Code=3201/System Code=2722/Credential Number=693277/CS=1/ICI=5/PI=7241649364/OC=1/OI=3201/POA=1)

URI:urn:uuid:6c4ecd74-88c4-4828-9521-4902c8b4687c

D.4.15.3 Test PIV Card 15: Digital Signature Certificate

Status: revoked

Serial Number: 1503 (0x5df)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

2E:76:EC:87:74:0D:5D:14:D8:52:C2:E4:F0:7D:19:BF:6D:40:C0:87

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.4 Test PIV Card 15: Key Management Certificate

Status: revoked

Serial Number: 1504 (0x5e0)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

02:41:B3:13:87:02:C8:D5:68:EF:3A:A5:B0:D0:17:BC:66:5F:6B:46

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.5 Test PIV Card 15: Retired Key Management Certificate A

Serial Number: 1505 (0x5e1)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Nov 17 17:23:14 2006 GMT, Not After: Nov 17 17:23:14 2008 GMT

Subject: CN=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 1024-bit modulus, e=65537

Extensions:

Authority Key Identifier:

15:40:EC:5B:D2:37:35:34:01:1E:3D:2E:04:C1:5F:5E:2F:55:02:F6

Subject Key Identifier:

9A:54:B6:9D:93:AB:02:B1:F3:F8:AA:EB:67:44:98:15:13:2A:EA:7C

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://p7c.example.com/PIVTest/CACertsIssuedToRSA1024CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.6 Test PIV Card 15: Retired Key Management Certificate B

Serial Number: 1506 (0x5e2)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2007 GMT, Not After: Apr 3 19:56:01 2009 GMT

Subject: CN=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

0E:1E:EB:B0:C0:8F:1E:E8:A6:3B:52:6C:38:D4:52:FF:CD:6A:7A:79

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.7 Test PIV Card 15: Retired Key Management Certificate C

Serial Number: 1507 (0x5e3)

Signature Algorithm: sha1WithRSAEncryption

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

Validity: Not Before: Apr 3 19:56:01 2008 GMT, Not After: Apr 3 19:56:01 2010 GMT

Subject: CN=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

78:85:E1:08:24:11:82:3A:34:41:59:94:D4:80:BF:23:EB:06:C9:1B

Subject Key Identifier:

19:A6:D2:91:F3:37:A8:F8:BB:F0:6E:02:0B:85:B2:A6:8E:93:BC:AB

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToExpiredRSA2048CA.p7c

CA Issuers - 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

OCSP - http://ocsp.example.com

Key Usage: critical

Key Encipherment

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.8 Test PIV Card 15: Retired Key Management Certificate D

Serial Number: 1508 (0x5e4)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Sep 25 23:18:12 2008 GMT, Not After: Sep 25 23:18:12 2010 GMT

Subject: CN=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

61:30:9F:04:34:71:DE:44:FC:F3:AA:8F:31:20:4C:D4:89:E3:78:3F

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.9 Test PIV Card 15: Retired Key Management Certificate E

Serial Number: 1509 (0x5e5)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Mar 12 02:04:01 2009 GMT, Not After: Mar 12 02:04:01 2011 GMT

Subject: CN=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

9F:50:2C:47:8C:5E:75:B2:C0:F3:DC:0D:61:B7:26:74:77:13:B4:71

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.10 Test PIV Card 15: Retired Key Management Certificate F

Serial Number: 1504 (0x5e0)

Signature Algorithm: ecdsa-with-SHA256

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

Validity: Not Before: Oct 1 08:30:00 2010 GMT, Not After: Oct 1 08:30:00 2030 GMT

Subject: CN=Test E. Cardholder XV, ou=Test Agency, ou=Test Department, o=Test Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

F0:C8:42:B4:82:B4:9D:0E:46:F7:CC:21:D4:9C:51:8B:DC:46:F9:ED

Subject Key Identifier:

B2:BE:E0:D2:D4:99:E4:2E:BC:FC:EF:05:D9:A2:8A:41:8B:4E:10:8B

CRL Distribution Points:

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

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

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest/CACertsIssuedToECCP-256CA.p7c

CA Issuers - 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

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.15.11 Test PIV Card 15: Retired Key Management Certificate G

Serial Number: 1505 (0x5e1)

Signature Algorithm: ecdsa-with-SHA256

Issuer: CN=Test ECC P-256 CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2016 GMT, Not After: Aug 5 08:30:00 2019 GMT

Subject: CN=Test Cardholder XV, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: id-ecPublicKey, P-256

Extensions:

Authority Key Identifier:

77:6E:68:4A:1D:98:AF:46:CD:26:90:96:28:C3:E4:FD:CD:55:79:2C

Subject Key Identifier:

0F:F8:9D:78:95:1B:66:9A:88:5A:59:39:4B:D3:AB:C4:39:8D:49:E8

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/ECCP256IssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToECCP256IssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20ECC%20P-256%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Agreement

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_fpki_common_hardware

Subject Alternative Name:

email:test.cardholder15@mail.example.com

D.4.16 Test PIV Card 16

D.4.16.1 Test PIV Card 16: PIV Authentication Certificate

Status: not revoked

Serial Number: 1601 (0x641)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XVI, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

Subject Key Identifier:

73:0D:32:2C:A2:E8:55:76:D6:5C:38:26:18:77:CD:C4:1A:9F:D0:0E

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048PIV-IIssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048PIV-IIssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage:

TLS Web Client Authentication, Microsoft Smartcard Login, PKINIT Client Auth

Certificate Policies:

id_pivi_issuer_certpcy_hardware

Subject Alternative Name:

UPN:pivitestcardholder@upn.example.com

URI:urn:uuid:e51faf01-14d7-471d-83e1-69e5d725ba64

D.4.16.2 Test PIV Card 16: Card Authentication Certificate

Status: not revoked

Serial Number: 1602 (0x642)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: serialNumber=e51faf01-14d7-471d-83e1-69e5d725ba64, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

Subject Key Identifier:

BA:98:A1:95:EA:53:3E:7A:C8:66:EE:F0:6D:D2:2F:2E:39:B8:C5:91

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048PIV-IIssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048PIV-IIssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature

Extended Key Usage: critical

id_piv_cardAuth

Certificate Policies:

id_pivi_issuer_certpcy_cardAuth

Subject Alternative Name:

URI:urn:uuid:e51faf01-14d7-471d-83e1-69e5d725ba64

D.4.16.3 Test PIV Card 16: Digital Signature Certificate

Status: not revoked

Serial Number: 1603 (0x643)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XVI, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

Subject Key Identifier:

A7:16:70:77:ED:C6:C9:30:6F:BC:A3:C3:D1:BA:D5:C5:40:25:47:43

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048PIV-IIssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048PIV-IIssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Digital Signature, Non-Repudiation

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_pivi_issuer_certpcy_hardware

Subject Alternative Name:

email:test.cardholder16@mail.example.com

D.4.16.4 Test PIV Card 16: Key Management Certificate

Status: not revoked

Serial Number: 1604 (0x644)

Signature Algorithm: sha256WithRSAEncryption

Issuer: CN=Test PIV-I RSA 2048-bit CA for Test PIV Cards v2, ou=Test CA, o=Test Certificates 2020, c=US

Validity: Not Before: Aug 5 08:30:00 2019 GMT, Not After: Dec 31 08:30:00 2040 GMT

Subject: CN=Test Cardholder XVI, ou=Test Agency, ou=Test Department, o=U.S. Government, c=US

Subject Public Key Info: rsaEncryption, 2048-bit modulus, e=65537

Extensions:

Authority Key Identifier:

36:DC:7B:64:B8:56:FB:0E:BF:AA:06:A6:F8:93:27:99:47:B6:B3:8A

Subject Key Identifier:

F6:12:FA:CC:5A:9B:A7:78:0B:9A:68:D3:21:0B:81:D9:CC:D0:08:43

CRL Distribution Points:

http://smime2.nist.gov/PIVTest2/RSA2048PIV-IIssuingCA.crl

ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?certificateRevocationList;binary

Authority Information Access:

CA Issuers - http://smime2.nist.gov/PIVTest2/CACertsIssuedToRSA2048PIV-IIssuingCA.p7c

CA Issuers - ldap://smime2.nist.gov/cn=Test%20PIV-I%20RSA%202048-bit%20CA%20for%20Test%20PIV%20Cards%20v2,ou=Test%20CA,o=Test%20Certificates%202020,c=US?cACertificate;binary,crossCertificatePair;binary

OCSP - http://seclab7.ncsl.nist.gov

Key Usage: critical

Key Encipherment

Extended Key Usage:

E-mail Protection

Certificate Policies:

id_pivi_issuer_certpcy_hardware

Subject Alternative Name:

email:test.cardholder16@mail.example.com