NISTIR 7870

NIST Test Personal Identity Verification (PIV) Cards

David A. Cooper

http://dx.doi.org/10.6028/NIST.IR.7870

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

NISTIR 7870

NIST Text Personal Identity Verification (PIV) Cards

David A. Cooper
Computer Security Division
Information Technology Laboratory

http://dx.doi.org/10.6028/NIST.IR.7870

July 2012

U.S. Department of Commerce
Rebecca M. Blank, Acting Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, Under Secretary of Commerce for Standards and Technology and Director

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 analysis to advance the development and productive use of information technology. ITL's responsibilities include the development of technical, physical, administrative, and management standards and guidelines for the cost-effective security and privacy of sensitive unclassified information in Federal computer systems. This Interagency Report discusses ITL's research, guidance, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.

National Institute of Standards and Technology Interagency Report
12 pages (2012)

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. 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 and the infrastructure that has been developed to support their use.

Disclaimer

Statements made in this paper are the opinions of the author and should not be interpreted as standards, guidelines, best practices, or recommendations for specific changes to any other NIST publications.

Table of Contents

1. Introduction

In order to facilitate the development of applications and middleware that support the Personal Identity Verification (PIV) Card, NIST has developed a set of test PIV Cards 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 include examples of certificates and data objects that are signed using each of the algorithms and key sizes listed in Table 3-3 of SP 800-78-3, including RSASSA-PSS and ECDSA. Similarly, the infrastructure supporting the test cards provides examples of 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 ECC subject public keys in addition to RSA subject public keys, as is permitted by Table 3-1 of SP 800-78-3. The set of test cards, collectively, also include all of the mandatory and optional data objects listed in Section 3 of SP 800-73-3 Part 1, except for Cardholder Iris Images. Several of the cards include a Key History object along with retired key management keys.

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 http://csrc.nist.gov/groups/SNS/piv/testcards.html.

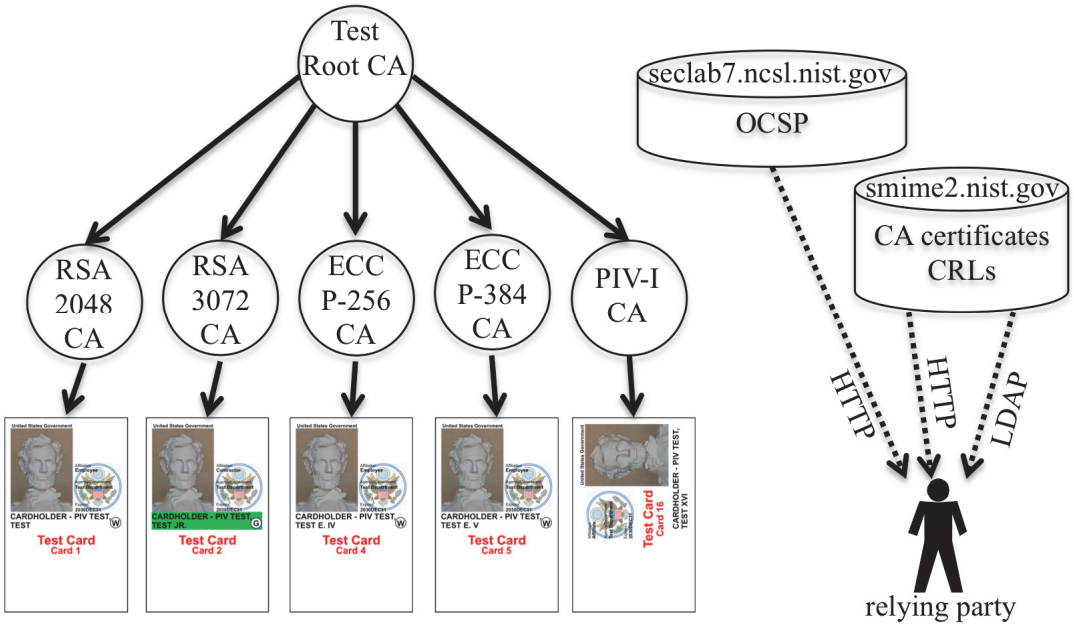

Figure 1 – PKI for Test PIV Cards

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 both HTTP and LDAP URIs that point to the relevant CRL for that certificate. Each of these certificates also includes an authorityInfoAccess extension with both HTTP and LDAP URIs that point to the location where the CA certificates issued to the issuer of the certificate may be found. Each CA certificate issued by the PKI, including 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 subject of the certificate may be found. While some certificate validation software will be able to 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 http://csrc.nist.gov/groups/SNS/piv/testcards.html.

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. Each of the CAs issues CRLs once an hour, with the CRLs specifying a nextUpdate time that is 24 hours after the CRL was issued. The OCSP responder only provides pre-signed responses, which are also produced once an hour. The nextUpdate time indicated for each certificate in the OCSP responses is 2 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. 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 based on the PIV Cards that are currently issued by the U.S. General Services Administration's USAccess program (http://www.fedidcard.gov), which issues PIV Cards for many federal agencies. Test PIV Card 1 contains many of the optional data objects specified in SP 800-73-2, but none of the data objects that were newly specified in SP 800-73-3. 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 and smart card logon object identifiers (OIDs) in addition to the anyExtendedKeyUsage OID.

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 user principal name (UPN) in the subjectAltName extension and does not include an extended key usage 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. In addition, Test PIV Card 2 includes a Key History object, but the Key History object merely indicates that no retired keys are present on the card.

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 anyExtendedKeyUsage OIDs, but not the smart card logon OID. 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. The GUID data element of the CHUID contains a UUID, and this UUID is also included in the PIV Authentication certificate, the Card Authentication certificate, and the signed data objects, as specified in SP 800-73-3. 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 three retired key management keys on the card (one 1024-bit RSA key and two 2048-bit RSA keys) and that the corresponding certificates for all three 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 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.[1] While the PIV Authentication certificate includes a UPN in the subjectAltName extension, it does not include an extended key usage 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 five retired key management keys on the card (three 2048-bit RSA keys and two ECC Curve P-256 keys) and that the certificates corresponding to three 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 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 an extended key usage extension and does not include any name forms in the subjectAltName extension other than the FASC-N. The GUID data element of the CHUID contains an IPv6 address rather than all zeros. Test PIV Card 5 includes a Key History object that indicates that there are five retired key management keys on the card (two 2048-bit RSA, two ECC Curve P-256, one ECC Curve P-384), but that

[1] A few of the retired certificates for key management contain RSA subject public keys and are signed using RSA PKCS #1 v1.5.

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 6:

Test PIV Card 6 only contains those data objects that are listed as mandatory in SP 800-73-3 (except for the Discovery object, which is present on every test card). Test PIV Card 6 includes a PIV Authentication certificate, but no Card Authentication certificate, 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 PIV Authentication certificate only includes the card's FASC-N. The PIV Authentication certificate does not include an extended key usage extension. 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. Neither the Cardholder Facial Image nor the Printed Information buffer is present on the card.

Test PIV Card 7:

Test PIV Card 7 represents a legacy PIV Card by using RSA PKCS #1 v1.5 with SHA-1 rather than RSA PKCS #1 v1.5 with SHA-256 to sign the certificates and data objects on the card. In addition, the PIV Authentication and Card Authentication keys are 1024-bit RSA rather than 2048-bit RSA. Like Test PIV Card 1, the PIV Authentication certificate on Test PIV Card 7 includes a UPN in the subjectAltName extension and includes an extended key usage extension that asserts the client authentication, smart card logon, and anyExtendedKeyUsage OIDs. 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 five retired key management keys on the card (one 1024-bit RSA key and four 2048-bit RSA keys) and that the certificates corresponding to three 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:

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, but the extended key usage extension does not assert the smart card logon OID. Instead the extended key usage extension includes OIDs for TLS client authentication, PKINT client authentication, EAP over PPP, EAP over LAN, and anyExtendedKeyUsage. 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 ten retired key management keys on the card (two 1024-bit RSA and eight 2048-bit RSA) and that the certificates corresponding to three 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 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 five retired key management keys on the card (all 2048-bit RSA keys) and that the certificate corresponding to one of these keys is 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 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 in the CHUID does not match the FASC-N in the biometric data objects or in the authentication certificates. If PIV biometric authentication were performed as specified in Section 6.2.3.1 of FIPS 201-1, 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 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. Like Test PIV Card 7, the PIV Authentication and Card Authentication keys are 1024-bit RSA and all four of the cardholder's certificates were signed using RSA PKCS #1 v1.5 with SHA-1.

Test PIV Card 14:

On Test PIV Card 14, the certificate corresponding 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 five retired key management keys on the card (all 2048-bit RSA) and that the certificate corresponding to one of the keys is 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:

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 five retired key management keys on the card (one 1024-bit RSA, two 2048-bit RSA, and two ECC Curve P-256) and that the certificates corresponding to three 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 16:

Test PIV-I Card 16 represents a PIV-I Card rather than a PIV Card. The GUID data element of the CHUID contains a UUID and the FASC-N data element of the CHUID contains a value that indicates that the card is a PIV-I card. The UUID from the GUID data element is included in the signed data objects and in the authentication certificates instead of the FASC-N, as specified in SP 800-73-3.

Appendix A—Acronyms

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

Appendix B—References

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

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

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

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