NISTIR 7676

Maintaining and Using Key History on Personal Identity Verification (PIV) Cards

David A. Cooper

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

NISTIR 7676

Maintaining and Using Key History on Personal Identity Verification (PIV) Cards

David A. Cooper

Computer Security Division
Information Technology Laboratory

June 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick D. Gallagher, 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
15 pages (2010)

Abstract

NIST Special Publication 800-73-3 [7] introduces the ability to store retired Key Management Keys within the Personal Identity Verification (PIV) Card Application on a PIV Card. This paper complements SP 800-73-3 by providing some of the rationale for the design of the mechanism for storing retired Key Management Keys on PIV Cards and by providing suggestions to smart card vendors, PIV Card Issuers, and middleware developers on the use of the Key History mechanism.

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

Federal Information Processing Standard (FIPS) 201 [2] specifies that a PIV Card may include a Key Management Key to support either key transport or key agreement. This key may be used to enable the encryption of data to protect the data while it is being sent across a network and while it is at rest. For example, an email message may be encrypted by the sender to protect the message from eavesdropping while it is being sent and the encrypted email may be stored on the recipient's computer or mail server to be decrypted each time the recipient reads the email.

Each Key Management Key has a limited lifetime and must be replaced periodically with a newly generated key pair. While any newly encrypted data should be encrypted using the most recently generated Key Management public key, users need to continue to have access to their older Key Management private keys to be able to decrypt data that has been stored in encrypted form and that was encrypted using one of their older Key Management public keys.

Special Publication 800-73-3 [7] provides for the ability to store these older (retired) Key Management Keys within the PIV Card Application. The storage and use of retired Key Management Keys on a PIV Card involves a number of tradeoffs. In order to decrypt an encrypted message, an application needs access to information that will allow it to determine which private key to use to perform the decryption. Thus, in addition to the private key, some additional information needs to be made available to applications to aid in identifying the appropriate private key to use to perform a decryption operation. If insufficient information is made available to applications, then applications may be unable to make use of the private keys. However, storage space on PIV Cards is limited and reading data from a PIV Card can be relatively slow, so there is a need to avoid storing more information than necessary on the card.

This paper describes the mechanism in SP 800-73-3 that supports the maintenance of key history within the PIV Card Application and provides suggestions to PIV Card manufacturers, issuers, and middleware developers on the use of the Key History mechanism. Readers of this paper should be familiar with the description of the Key History mechanism in Part 1 of SP 800-73-3.

2. Overview

FIPS 201 [2] specifies one mandatory and three optional asymmetric key pairs that may appear on PIV Cards: the PIV Authentication Key, the Card Authentication Key, the Digital Signature Key, and the Key Management Key. FIPS 201 requires that whenever one of these keys is present on the card, the corresponding X.509 certificate [6] must also be stored on the card. Storing the certificates on the card ensures that any application that has access to the private keys also has access to the corresponding certificates. In the case of the Key Management Key, it is likely that the only information about the cardholder's Key Management Key that an entity encrypting a message intended for the cardholder will use will be the X.509 certificate containing the public key. Ensuring that the PIV Card-using application also has access to the certificate ensures that the application will have access to all the information that it needs to determine whether the Key Management Key on the PIV Card was used to encrypt a particular encrypted message.

In most cases, an encrypted message does not include a copy of the certificate whose public key was used to encrypt the data. For example, a common format for encrypted data that will be stored in encrypted form is the envelopedData content type of the Cryptographic Message Syntax (CMS) [8], which is used in S/MIME to encode encrypted email messages. In CMS, the public key that was used to encrypt the message is identified by specifying either the contents of the subjectKeyIdentifier extension from the certificate from which the key was taken or the issuer distinguished name and serial number from the certificate. The recipient must then identify the private key corresponding to the certificate that contains this information in order to decrypt the message.

While storing the certificates corresponding to retired Key Management private keys on the PIV Card ensures that they are always accessible to PIV Card-using applications that may need them, there are two drawbacks: the storage space that would be needed to hold the certificates may be needed for other purposes and it may take too long to read all of the certificates from the PIV Card. SP 800-73-3 [7] addresses these issues by allowing the entity that loads the PIV Card Application onto a PIV Card to decide how much space to allocate on the PIV Card to the storage of retired X.509 certificates for Key Management and by enabling access to these certificates from an off-card source. When the PIV Card-using application can access retired certificates from an off-card source, the application does not need to read them from the card. The certificates that are stored on the PIV Card may serve as an alternative source for the certificates for PIV Card-using applications that cannot obtain the certificates from an off-card source.

This paper assumes that applications will only make use of Key Management private keys if they have access to the corresponding certificates. This would mean that a PIV Card-using application that cannot access the off-card certificate source would be limited to using the retired Key Management private keys for which the corresponding certificates are stored within the PIV Card Application. A PIV Card-using application that did not have access to the certificate containing the public key that was used to encrypt a message could try to decrypt the message with every private key in its possession until it had either successfully decrypted the message or had tried every private key, but this paper assumes that applications will not do this.

3. Storing Retired Keys Within the PIV Card Application

SP 800-73-3 [7] allows for up to twenty retired Key Management Keys to be stored within the PIV Card Application on a PIV Card. SP 800-73-3 imposes a limit of twenty retired Key Management Keys since ISO/IEC 7816-4 [3] requires each key to be assigned a unique key reference value and limits each card application to thirty-two different key reference values. Seven of the PIV Card Application's key reference values have already been assigned to other keys (PIV Card Application PIN ['80'], PIN Unblocking Key ['81'], PIV Authentication Key ['9A'], Card Management Key ['9B'], Digital Signature Key ['9C'], Key Management Key ['9D'], and Card Authentication Key ['9E']). The remaining five key reference values for the PIV Card Application are being reserved for possible future use.

When the PIV Card Application is loaded onto a card, space may be allocated for zero to twenty retired Key Management private keys and their corresponding certificates. Space may be allocated for fewer certificates than private keys. Where space on the card is limited, it is recommended that priority be given to allocating space for as many retired Key Management private keys as possible while also allocating space for at least one retired X.509 certificate for Key Management. Storing at least one certificate on the card will ensure that the most recently retired Key Management Key will always be available for use, even when the PIV Card-using application cannot access the off-card certificate source. Maximizing the number of retired Key Management private keys stored on the card will ensure maximal availability of older encrypted data whenever the PIV Card-using application has access to all of the corresponding certificates.

When all of the retired X.509 certificates for Key Management are stored within the PIV Card Application, SP 800-73-3 does not require those certificates to also be available from an off-card source. However, it is recommended that issuers make retired certificates available from an off-card source even in this case since it will generally be much faster for the PIV Card-using application to obtain the certificates from an off-card source than to read them from the PIV Card.

When retired certificates are made available from an off-card source, the URL that points to the off-card source must be of the form:

"http://" <DNS name> "/" <ASCII-HEX encoded SHA-256 hash of **OffCardKeyHistoryFile**>

For example, the *offCardCertURL* that points to the sample **OffCardKeyHistoryFile** shown in Appendix A is

http://smime2.nist.gov/8B0F34EA6AFC8322CE557CCEF49A8327CDAC58D67405CEFDE0A05E01895BFF46

The *offCardCertURL* is included in the Key History object, which is protected by the digitally signed Security Object. This allows the PIV Card-using application to verify the integrity of the SHA-256 hash [1] that is encoded in the *offCardCertURL*. The SHA-256 hash serves three purposes:

1. It allows the PIV Card-using application to verify the contents of the **OffCardKeyHistoryFile** by comparing a hash of the downloaded file to the hash value encoded in the URL.
2. It supports local caching of the **OffCardKeyHistoryFile** by providing a simple mechanism for ensuring that a locally cached file exactly matches the file referenced by the URL on a PIV Card. Locally caching the **OffCardKeyHistoryFile** after it is downloaded the first time allows for faster access to the retired certificates during subsequent uses of the PIV Card and ensures access to the retired certificates that are not

stored within the PIV Card Application even if the PIV Card-using application is not connected to the network or the server holding the **OffCardKeyHistoryFile** is temporarily unavailable.

3. Encoding the SHA-256 hash of the **OffCardKeyHistoryFile** in the *offCardCertURL* ensures that the URL cannot be guessed by anyone who does not already have access to the **OffCardKeyHistoryFile** or to the PIV Card.

If the server holding the certificates does not allow users to obtain a listing of the files in a directory, making the URLs unguessable should prevent anyone who is not in possession of a PIV Card from downloading the **OffCardKeyHistoryFile** referenced by the card even though the file can be downloaded by anyone who knows the file's URL. Since X.509 certificates for Key Management may be publicly distributed, configuring the server to prevent users from obtaining a listing of the files in a directory should provide a sufficient level of protection against the off-card certificate files being downloaded by anyone who is not in possession of the PIV Card. However, since the retired X.509 certificates for Key Management are only needed by the cardholder, Agencies may choose to place the server holding the off-card certificate files on an internal network, although doing so may cause problems for cardholders trying to use their PIV Cards while they are telecommuting or on travel.

A new **OffCardKeyHistoryFile** will need to be created whenever a new Key Management Key is created for a cardholder and the cardholder's previous Key Management Key is moved into the key history.[1] Since the SHA-256 hash of the **OffCardKeyHistoryFile** is encoded in the *offCardCertURL*, the *offCardCertURL* in a PIV Card's Key History object will need to be updated whenever a new **OffCardKeyHistoryFile** is created for the card. Moving a newly retired Key Management Key into the key history may also result in the value of either *keysWithOnCardCerts* or *keysWithOffCardCerts* needing to be changed. Whenever any of the values within the Key History object are changed, the hash of the Key History object in the Security Object will need to be updated and the Security Object will need to be re-signed.

As a general rule, PIV Card-using applications that may need access to retired X.509 certificates for Key Management should first read the Key History object. If the Key History object is present and contains an *offCardCertURL*, then the PIV Card-using application should look for the **OffCardKeyHistoryFile** that is referenced by the *offCardCertURL* in a local cache. If the file cannot be found there, or if there is no local cache, the PIV Card-using application should use the *offCardCertURL* to download the **OffCardKeyHistoryFile** from the server. Whether the **OffCardKeyHistoryFile** is obtained from the local cache or from a remote server, the SHA-256 hash of the file should be compared with the SHA-256 hash encoded in the *offCardCertURL* to ensure that the correct file has been obtained. PIV Card-using applications should be prepared for the possibility that the server holding the **OffCardKeyHistoryFile** cannot be accessed even if network connectivity is available since the server may only be available from an Agency's internal network. If the Key History object does not include an *offCardCertURL* or if the **OffCardKeyHistoryFile** referenced by the *offCardCertURL* is not locally cached and cannot be downloaded from the server, then the PIV Card-using application will need to read the retired X.509 certificates for Key Management from the PIV Card, if they have been stored on the card. The PIV Card-using application does not need to validate the retired X.509 certificates for Key Management since they are only being used to aid in identifying the appropriate private key to use to decrypt data that was previously encrypted.

[1] An **OffCardKeyHistoryFile** does not need to be created if all of the retired X.509 certificates for Key Management are stored within the PIV Card Application and the *offCardCertURL* is omitted from the PIV Card's Key History object.

If a PIV Card-using application is unable to access the **OffCardKeyHistoryFile**, then the application will only be able to make use of the retired Key Management Keys for which the corresponding certificates are also stored on the PIV Card. The design of the Key History mechanism takes this into consideration. In general, a given retired Key Management Key's use will decline with age. So, PIV Card-using applications will typically need access to the most recently retired Key Management Keys more frequently than they will need access to older retired Key Management Keys. Thus, SP 800-73-3 requires that if the PIV Card does not store all of the retired X.509 certificates for Key Management then the card must store those certificates corresponding to the most recently issued Key Management Keys.

Tables 1 through 4 provide examples of the storage of retired Key Management Keys within the PIV Card Application. All four examples involve the storage of the same set of seven retired keys, but the examples differ in the number of retired X.509 certificates for Key Management that are stored within the PIV Card Application. For each retired Key Management private key that is stored within the PIV Card Application, the tables show the key reference value assigned to the private key, the BER-TLV tag for the corresponding certificate (if the certificate is stored within the PIV Card Application), the date when the certificate was issued (notBefore), and the date when the certificate expires (notAfter).

Note that in the examples, each of the Key Management Keys was replaced with a newer key long before the end of the corresponding certificate's three-year lifespan. While a cardholder would not typically be issued new Key Management Keys so frequently, a cardholder may be issued a new Key Management Key well before the end of the current Key Management Key's certificate's lifetime if the PIV Card was lost or broken, information in the certificate (e.g., email address) needed to be changed, or the PIV Card needed to be replaced as a result of changes in information printed on the face of the card (e.g., rank).

Table 1 presents an example in which all of the certificates are stored within the PIV Card Application. Since *keysWithOffCardCerts* is zero, the *offCardCertURL* is not required to be present in the Key History object. In order to facilitate discovery of the key references and BER-TLV tags that correspond to the retired private keys and certificates, respectively, SP 800-73-3 requires that the retired keys be assigned key references '82' through '88' and that the certificates be stored in the BER-TLV tags that correspond to these key references. However, there is no requirement with respect to which retired key is assigned to which of these key references. Thus, in this example, the keys have been assigned to key references '82' through '88' at random.

Table 2 presents an example in which only four of the seven retired X.509 certificates for Key Management are stored within the PIV Card Application. In this case, the *offCardCertURL* is required to be present and the file that is referred to by the URL must contain all seven of the retired X.509 certificates for Key Management (see Appendix A). As is required by SP 800-73-3, the four retired Key Management Keys that were most recently issued are the ones that are stored within the PIV Card Application. These certificates must be stored in BER-TLV tags '5FC10D' through '5FC110'. The corresponding private keys must be assigned to the corresponding key references as specified in Table 6 of SP 800-73-3, Part 1. For example, the private key corresponding to the certificate in BER-TLV tag '5FC10D' must be assigned key reference '82'. The oldest three private keys, the ones for which the corresponding certificates are not stored within the PIV Card Application, must be assigned key references '93' through '95'.

Tables 5 and 6 present two more examples of the storage of retired Key Management Keys within the PIV Card Application. Both examples are based on a scenario in which the PIV Card Application is holding the seven retired Key Management Keys depicted in the examples in Tables 1 though 4 and the cardholder is issued a new Key Management Key, resulting in the previous Key Management Key becoming a retired Key Management Key. As in the example in

Table 3, the PIV Card Application only stores three retired X.509 certificates for Key Management.

Table 1: keysWithOnCardCerts = 7, keysWithOffCardCerts = 0

Key Reference	82	83	84	85	86	87	88
Certificate Tag	5FC10D	5FC10E	5FC10F	5FC110	5FC111	5FC112	5FC113
Cert. notBefore	03/08	11/05	05/05	05/07	10/06	01/09	04/07
Cert. notAfter	03/11	11/08	05/08	05/10	10/09	01/12	04/10

Table 2: keysWithOnCardCerts = 4, keysWithOffCardCerts = 3

Key Reference	82	83	84	85	93	94	95
Certificate Tag	5FC10D	5FC10E	5FC10F	5FC110	N/A	N/A	N/A
Cert. notBefore	03/08	01/09	05/07	04/07	05/05	10/06	11/05
Cert. notAfter	03/11	01/12	05/10	04/10	05/08	10/09	11/08

Table 3: keysWithOnCardCerts = 3, keysWithOffCardCerts = 4

Key Reference	82	83	84	92	93	94	95
Certificate Tag	5FC10D	5FC10E	5FC10F	N/A	N/A	N/A	N/A
Cert. notBefore	01/09	05/07	03/08	10/06	04/07	11/05	05/05
Cert. notAfter	01/12	05/10	03/11	10/09	04/10	11/08	05/08

Table 4: keysWithOnCardCerts = 0, keysWithOffCardCerts = 7

Key Reference	8F	90	91	92	93	94	95
Certificate Tag	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Cert. notBefore	10/06	05/05	04/07	05/07	01/09	03/08	11/05
Cert. notAfter	10/09	05/08	04/10	05/10	01/12	03/11	11/08

Table 5: keysWithOnCardCerts = 3, keysWithOffCardCerts = 4

Key Reference	82	83	84	92	93	94	95
Certificate Tag	5FC10D	5FC10E	5FC10F	N/A	N/A	N/A	N/A
Cert. notBefore	01/09	05/09	03/08	10/06	04/07	11/05	05/07
Cert. notAfter	01/12	05/12	03/11	10/09	04/10	11/08	05/10

Table 6: keysWithOnCardCerts = 3, keysWithOffCardCerts = 5

Key Reference	82	83	84	91	92	93	94	95
Certificate Tag	5FC10D	5FC10E	5FC10F	N/A	N/A	N/A	N/A	N/A
Cert. notBefore	01/09	05/09	03/08	05/07	10/06	04/07	11/05	05/05
Cert. notAfter	01/12	05/12	03/11	05/10	10/09	04/10	11/08	05/08

In the example in Table 5, the PIV Card Application is only capable of storing seven retired Key Management private keys. In this case, in order to make room for the new retired Key Management Key (associated with the certificate issued 05/09), the oldest retired Key Management Key (associated with the certificate issued 05/05) is removed from the PIV Card Application. Since the three most recently issued retired X.509 certificates for Key Management must be stored within the PIV Card Application, the certificate that was issued in May 2007 is also removed from the PIV Card Application in order to make room for the newly retired

certificate that was issued in May 2009. Since the certificate that was issued in May 2007 is no longer stored within the PIV Card Application, its corresponding private key must be assigned a key reference between '92' and '95' rather than a key reference between '82' and '84'.

In the example in Table 6, the PIV Card Application is capable of storing at least eight retired Key Management Keys, so no keys need to be removed from the PIV Card Application. However, as in the example in Table 5, the certificate that was issued in May 2007 needs to be removed from the PIV Card Application in order to make room for the certificate that was issued in May 2009, and the private key corresponding to the certificate that was issued in May 2007 needs to be assigned a key reference between '91' and '95' rather than a key reference between '82' and '84'.

Appendix A—Sample OffCardKeyHistoryFile

This appendix presents an example of the contents of the **OffCardKeyHistoryFile**, which is referenced by the *offCardCertURL* in the Key History object. The sample **OffCardKeyHistoryFile** corresponds to the example presented in Table 2. Examples corresponding to Tables 1, 3, and 4, would be nearly identical, with only the key references associated with each certificate being different.

The **OffCardKeyHistoryFile** contains the DER encoding [5] of the following ASN.1 [4]:

```
OffCardKeyHistoryFile ::= SEQUENCE SIZE (1..20) OF SEQUENCE {
        keyReference        OCTET STRING (SIZE(1))
        cert                Certificate
}
```

where **cert** is a retired X.509 certificate for Key Management and **keyReference** is the key reference assigned to the corresponding private key. The example below shows the pseudo-ASN.1 of the data that is being encoded on the left and the ASCII-HEX encoded representation of the contents of the **OffCardKeyHistoryFile** on the right. In order to enhance readability, only the first fourteen octets of each of the X.509 certificates are shown, but otherwise the entire contents of the **OffCardKeyHistoryFile** are presented. Each of the retired X.509 certificates for Key Management differ in their serial numbers, validity dates, subject public keys, and signatures, but are generally the same otherwise and so the lengths of each of the certificates and the first fourteen octets of each of the certificates are the same. The one exception is the certificate that was issued in January 2009, which includes an elliptic curve cryptography subject public key rather than an RSA subject public key, which results in this certificate being 203 octets shorter than the other certificates.

pseudo-ASN.1	**DER encoding**
OffCardKeyHistoryFile ::=	
SEQUENCE SIZE (7) OF	30 82 2E 6E
SEQUENCE	30 82 06 BB
keyReference // ('85')	04 01 85
cert // (issued 04/07)	30 82 06 B4 30 82 05 9C A0 03 02 01 02 02 …
SEQUENCE	30 82 06 BB
keyReference // ('82')	04 01 82
cert // (issued 03/08)	30 82 06 B4 30 82 05 9C A0 03 02 01 02 02 …
SEQUENCE	30 82 05 F0
keyReference // ('83')	04 01 83
cert // (issued 01/09)	30 82 05 E9 30 82 04 D1 A0 03 02 01 02 02 …
SEQUENCE	30 82 06 BB
keyReference // ('94')	04 01 94
cert // (issued 10/06)	30 82 06 B4 30 82 05 9C A0 03 02 01 02 02 …
SEQUENCE	30 82 06 BB
keyReference // ('93')	04 01 93
cert // (issued 05/05)	30 82 06 B4 30 82 05 9C A0 03 02 01 02 02 …
SEQUENCE	30 82 06 BB
keyReference // ('84')	04 01 84
cert // (issued 05/07)	30 82 06 B4 30 82 05 9C A0 03 02 01 02 02 …
SEQUENCE	30 82 06 BB
keyReference // ('95')	04 01 95
cert // (issued 11/05)	30 82 06 B4 30 82 05 9C A0 03 02 01 02 02 …

Appendix B—Acronyms

ASCII	American Standard Code for Information Interchange
ASN.1	Abstract Syntax Notation One
CMS	Cryptographic Message Syntax
DER	Distinguished Encoding Rules
DNS	Domain Name System
FIPS	Federal Information Processing Standard
HEX	Hexadecimal
HTTP	Hypertext Transfer Protocol
IEC	International Electrotechnical Commission
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
N/A	Not Applicable
NIST	National Institute of Standards and Technology
NISTIR	National Institute of Standards and Technology Interagency Report
PIV	Personal Identity Verification
RSA	Rivest, Shamir, Adleman cryptographic algorithm
SHA	Secure Hash Algorithm
S/MIME	Secure/Multipurpose Internet Mail Extensions
SP	Special Publication
URL	Uniform Resource Locator

Appendix C—References

[1] Federal Information Processing Standards Publication 180-3, *Secure Hash Standard (SHS)*, October 2008. (See http://csrc.nist.gov)

[2] Federal Information Processing Standards Publication 201-1, Change Notice 1, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, March 2006. (See http://csrc.nist.gov)

[3] ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*.

[4] ISO/IEC 8824-2:2008, *Information technology — Abstract Syntax Notation One (ASN.1): Information object specification*.

[5] ISO/IEC 8825-1:2008, *Information technology — ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)*.

[6] ISO/IEC 9594-8:2008, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks*.

[7] NIST Special Publication 800-73-3, *Interfaces for Personal Identity Verification – Part 1: End-Point PIV Card Application Namespace, Data Model and Representation*, February 2010. (See http://csrc.nist.gov)

[8] Russell Housley, *Cryptographic Message Syntax (CMS)*, Internet Engineering Task Force (IETF) Request for Comments (RFC) 5652, September 2009. (See http://www.ietf.org/rfc/rfc5652.txt)