NIST Special Publication 800-78-1
DRAFT

# Cryptographic Algorithms and Key Sizes for Personal Identity Verification

NIST
**National Institute of Standards and Technology**
Technology Administration
U.S. Department of Commerce

**W. Timothy Polk**
**Donna F. Dodson**
**William E. Burr**

I N F O R M A T I O N   S E C U R I T Y

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD, 20899-8930

***June 2006***

**U.S. Department of Commerce**
*Carlos M. Gutierrez, Secretary*

**National Institute of Standards and Technology**
*William Jeffrey, Director*

.

## NOTE FOR REVIEWERS

1. NIST has modified this Special Publication 800-78-1 to enhance interoperability, simplify the development of relying party applications, and enhance alignment with the National Security Agency's Suite B Cryptography. [SUITE B] Revision 1 reduces the set of elliptic curves approved for use with PIV cards and the supporting infrastructure from six curves to two. General and specific changes are listed in Appendix C, Errata, of this document.

2. Please submit your SP 800-78-1 comments using the comment template form provided on the http://www.csrc.nist.gov/piv-project/fips201-support-docs.html website.

3. Comments should be submitted to PIV_comments@nist.gov. Please include "Comments on Preliminary Draft SP 800-78-1 in the subject line."

4. The comment period closes at 5:00 EST (US and Canada) on October 2nd, 2006. Comments received after the comment period closes will be handled on as-time-is-available basis.

## 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 non-national security-related information in Federal information systems. This special publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

# Table of Contents

## List of Tables

# 1. Introduction

The Homeland Security Presidential Directive (HSPD) 12 mandated the creation of new standards for interoperable identity credentials for physical and logical access to Federal government locations and systems. Federal Information Processing Standard 201 (FIPS 201), *Personal Identity Verification (PIV) of Federal Employees and Contractors*, was developed to establish standards for identity credentials [FIPS201-1]. This document, Special Publication 800-78-1, specifies the cryptographic algorithms and key sizes for PIV systems and is a companion document to FIPS 201.

## 1.1 Authority

This document has been developed by the National Institute of Standards and Technology (NIST) in furtherance of its statutory responsibilities under the Federal Information Security Management Act (FISMA) of 2002, Public Law 107-347.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. This recommendation is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130, Section 8b(3), Securing Agency Information Systems, as analyzed in A-130, Appendix IV: Analysis of Key Sections. Supplemental information is provided A-130, Appendix III.

This recommendation has been prepared for use by Federal agencies. It may be used by non-governmental organizations on a voluntary basis and is not subject to copyright. Nothing in this document should be taken to contradict standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should this recommendation be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of OMB, or any other Federal official.

## 1.2 Purpose

FIPS 201 defines requirements for the PIV lifecycle activities including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201 also defines the structure of an identity credential that includes cryptographic keys. This document contains the technical specifications needed for the mandatory and optional cryptographic keys specified in FIPS 201 as well as the supporting infrastructure specified in FIPS 201 and the related Special Publications 800-73, *Interfaces for Personal Identity Verification* [SP800-73-1], and SP 800-76, *Biometric Data Specification for Personal Identity Verification* [SP800-76], that rely on cryptographic functions.

## 1.3 Scope

The scope of this recommendation encompasses the PIV Card, infrastructure components that support issuance and management of the PIV Card, and applications that rely on the credentials supported by the PIV Card to provide security services. The recommendation identifies acceptable symmetric and asymmetric encryption algorithms, digital signature algorithms, and message digest algorithms, and specifies mechanisms to identify the algorithms associated with PIV keys or digital signatures.

Algorithms and key sizes have been selected for consistency with applicable Federal standards and to ensure adequate cryptographic strength for PIV applications. All cryptographic algorithms employed in this specification provide at least 80 bits of security strength. For detailed guidance on the strength of cryptographic algorithms, see [SP800-57(1)], *Recommendation on Key Management – Part 1: General*.

## 1.4 Audience and Assumptions

This document is targeted at Federal agencies and implementers of PIV systems. Readers are assumed to have a working knowledge of cryptography and Public Key Infrastructure (PKI) technology.

## 1.5 Document Overview

The document is organized as follows:

+ Section 1, *Introduction*, provides the purpose, scope, audience, and assumptions of the document and outlines its structure.

+ Section 2, *Applications of Cryptography in FIPS 201*, identifies the cryptographic mechanisms and objects that employ cryptography as specified in FIPS 201 and its supporting documents.

+ Section 3, *On Card Cryptographic Requirements*, describes the cryptographic requirements for cryptographic keys and authentication information stored on the PIV Card.

+ Section 4, *Certificate Status Information*, describes the cryptographic requirements for status information generated by PKI Certificate Authorities (CAs) and Online Certificate Status Protocol (OCSP) responders.

+ Section 5, *PIV Card Management Keys*, describes the cryptographic requirements for management of information stored on the PIV Card.

+ Section 6, *Identifiers for PIV Card Interfaces*, specifies key reference values and algorithm identifiers for the application programming interface and card commands defined in [SP 800-73-1].

+ Appendix A, *Acronyms*, contains the list of acronyms used in this document.

+ Appendix B, *References*, contains the list of documents used as references by this document.

+ Appendix C, *Errata*, lists modifications since SP 800-78 was officially published.

## 2. Application of Cryptography in FIPS 201

FIPS 201 employs cryptographic mechanisms  to authenticate cardholders, secure information stored on the PIV Card, and secure the supporting infrastructure.

FIPS 201 and its supporting documents specify a suite of keys to be stored on the PIV Card for personal identity verification, digital signature generation, and key management.  The PIV cryptographic keys specified in FIPS 201 are:

+ The asymmetric PIV authentication key;
+ A card authentication key, which may be symmetric or asymmetric;
+ An asymmetric digital signature key for signing documents and messages; and
+ An asymmetric key management key, supporting key establishment or key transport.

The cryptographic algorithms, key sizes, and parameters that may be used for these keys are specified in Section 3.1.   PIV Cards must implement private key computations for one or more of the algorithms identified in this section.

Cryptographically protected objects specified in FIPS 201, SP 800-73, and SP 800-76 include:

+ The X.509 certificates for each asymmetric key on the PIV Card;
+ A digitally signed *Cardholder Unique Identifier* (CHUID);
+ Digitally signed biometrics using the Common Biometric Exchange Formats Framework (CBEFF) signature block; and
+ The SP 800-73 *Security Object*, which is a digitally signed hash table.

The cryptographic algorithms, key sizes, and parameters that may be used to protect these objects are specified in Section 3.2.  Certificate Authorities (CAs) and card management systems that protect these objects must support one or more of the cryptographic algorithms, key sizes, and parameters specified in Section 3.2.

Applications may be designed to use any or all of the cryptographic keys and objects stored on the PIV Card.  Where maximum interoperability is required, applications should support all of the identified algorithms, key sizes, and parameters specified in Sections 3.2 and 3.3.

FIPS 201 requires CAs and Online Certificate Status Protocol (OCSP) responders to generate and distribute digitally signed Certificate Revocation Lists (CRLs) and OCSP status messages. These revocation mechanisms support validation of the PIV Card, the PIV cardholder, the cardholder's digital signature key, and the cardholder's key management key.

The signed revocation mechanisms specified in FIPS 201 are:

+ X.509 CRLs that specify the status of a group of X.509 certificates; and
+ OCSP status response messages that specify the status of a particular X.509 certificate.

The cryptographic algorithms and key sizes, and parameters that may be used to sign these mechanisms are specified in Section 4. Section 4 also describes rules for encoding the signatures to ensure interoperability.

FIPS 201 permits optional card management operations. These operations may only be performed after the PIV Card authenticates the card management system. Card management systems are authenticated through the use of card management keys. The cryptographic algorithms and key sizes that may be used for these keys are specified in Section 5.

# 3. On Card Cryptographic Requirements

FIPS 201 identifies a suite of objects that are stored on the PIV Card for use in authentication mechanisms or in other security protocols. These objects may be divided into three classes: cryptographic keys, signed authentication information stored on the PIV Card, and message digests of information stored on the PIV Card. Cryptographic requirements for PIV keys are detailed in Section 3.1. Cryptographic requirements for other stored objects are detailed in Section 3.2.

## 3.1 PIV Cryptographic Keys

FIPS 201 specifies four different classes of cryptographic keys to be used as credentials by the PIV cardholder:

- The mandatory PIV authentication key;
- An optional card authentication key;
- An optional digital signature key; and
- An optional key management key.

Table 3-1 establishes specific requirements for cryptographic algorithms and key sizes for each key type. Table 3-1 also specifies two time periods with different sets of acceptable algorithms for each key type. Note that digital signature and key management keys must transition to larger key sizes by 2008, while authentication keys must transition by 2010. This requirement anticipates that digital signature and key management keys will be used to protect data for longer periods of time, while data enciphered solely for authentication is generally not retained, and should not include private or secret information.

In addition to the key sizes, keys must be generated using secure parameters. Rivest, Shamir, Adleman (RSA) keys must be generated using appropriate exponents, as specified in Table 3-2. Elliptic curve keys must correspond to one of the following recommended curves from [FIPS186-3]:

- Curve P-256; *or*
- Curve P-384.

A PIV Card that supports elliptic curve cryptography must support private key computations for one or more of the listed curves. Applications that rely upon the PIV Card to authenticate users may select which curves to implement based on the community of users.

Note that FIPS 186-3 specifies a set of fifteen recommended curves. This specification limits PIV cryptographic keys to two curves to promote interoperability. Since both curves have sufficient strength to remain secure after 2010, no phase out date is required.[1]

[1] Note that 1024 bit RSA is permitted to leverage current products and promote efficient adoption of FIPS 201, but must be phased out by 2010 for authentication keys and 2008 for digital signatures and key management.

**Table 3-1. Algorithm and Key Size Requirements for PIV Key Types**

| PIV Key Type | Time Period for Use | Algorithms and Key Sizes |
|---|---|---|
| PIV Authentication key | Through 12/31/2010 | RSA (1024 or 2048 bits)<br>ECDSA (Curves P-256 and P-384) |
| | After 12/31/2010 | RSA (2048 bits)<br>ECDSA (Curves P-256 and P-384) |
| Card Authentication key | Through 12/31/2010 | 2TDEA<br>3TDEA<br>AES-128, AES-192, and AES-256<br>RSA (1024 or 2048 bits)<br>ECDSA (Curves P-256 and P-384) |
| | After 12/31/2010 | 3TDEA<br>AES-128, AES-192, and AES-256<br>RSA (2048 bits)<br>ECDSA (Curves P-256 and P-384) |
| Digital Signature key | Through 12/31/2008 | RSA (1024 or 2048 bits)<br>ECDSA (Curves P-256 and P-384) |
| | After 12/31/2008 | RSA (2048 bits)<br>ECDSA (Curves P-256 and P-384) |
| Key Management key | Through 12/31/2008 | RSA key transport (1024 or 2048 bits)<br>ECDH or ECC MQV Curves P-256 and P-384) |
| | After 12/31/2008 | RSA key transport (2048 bits);<br>ECDH or ECC MQV (Curves P-256 and P-384) |

This specification also restricts the size of the RSA exponent that may be associated with PIV keys. Implementations of this specification must choose an exponent greater than or equal to 65,537. Upper bounds for the exponent are based on key length; see Table 3-2 for complete details.

**Table 3-2. RSA Public Key Exponents**

| RSA Modulus Size | Minimum exponent | Maximum exponent |
|---|---|---|
| 1024 | 65,537 ($2^{16} + 1$) | $2^{864} – 1$ |
| 2048 | 65,537 | $2^{1824} – 1$ |

This specification requires that the key management key must be an RSA key transport key, an Elliptic Curve Diffie-Hellman (ECDH) key, or an elliptic curve Menezes-Qu-Vanstone (MQV) key. The specification for RSA key transport is [PKCS1]; the specification for ECDH and elliptic curve MQV is [SP800-56A].

## 3.2 Authentication Information Stored on the PIV Card

### 3.2.1 Specification of Digital Signatures on Authentication Information

FIPS 201 requires the use of digital signatures to protect the integrity and authenticity of information stored on the card. FIPS 201 and SP 800-73 require digital signatures on the following objects stored on the PIV Card:

- The CHUID;
- Biometric information (e.g., fingerprints);
- the SP 800-73 Security Object; *and*
- X.509 public key certificates.

Approved Digital Signature algorithms are specified in [FIPS 186-3]. Table 3-3 provides specific guidance for digitally signed information stored on the PIV Card. The first column specifies two time periods; the remaining columns specify public key algorithms and hash algorithms for generating digital signatures. For signatures on the CHUID, 800-73 Security Object, and stored biometrics, the size of the public key and the hash algorithm that must be used to generate the signature is determined by the expiration date of the PIV Card. For X.509 certificates stored on the card, the size of the public key and the hash algorithm used to generate the signature is determined by the expiration date associated with the certificate. Agencies are cautioned that generating digital signatures with SHA-256 and SHA-384 may initially limit interoperability.

**Table 3-3. Signature Algorithm and Key Size Requirements for PIV Information**

| Card or Certificate Expiration Date | Public Key Algorithms and Key Sizes | Hash Algorithms | Padding Scheme |
|---|---|---|---|
| Through 12/31/2010 | RSA (1024, 2048, or 3072 bits) | SHA-1 or SHA-256 | PKCS #1 v1.5 |
| | RSA (1024, 2048, or 3072 bits) | SHA-256 | PSS |
| | ECDSA (Curve P-256) | SHA-256 | N/A |
| | ECDSA (Curve P-384) | SHA-384 | N/A |
| After 12/31/2010 | RSA (2048 or 3072 bits) | SHA-256 | PKCS #1 v1.5, PSS |
| | ECDSA (Curve P-256) | SHA-256 | N/A |
| | ECDSA (Curve P-384) | SHA-384 | N/A |

FIPS 201, SP 800-73, and SP 800-76 specify formats for the CHUID, the Security Object, the biometric information, and X.509 public key certificates which rely on object identifiers (OID) to specify which signature algorithm was used to generate the digital signature. The object identifiers specified in Table 3-4 must be used in FIPS 201 implementations to identify the signature algorithm. Note that RSA digital signatures may be generated using either the PKCS #1 v.1.5 padding scheme or the Probabilistic Signature Scheme (PSS) padding. Most current implementations of RSA use the padding scheme defined in PKCS #1 v.1.5. The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS1]). Implementations of this specification must use the SHA-256 hash algorithm when generating RSA-PSS signatures. Agencies may wish to transition to the PSS padding scheme as they transition to SHA-256.

**Table 3-4. FIPS 201 Signature Algorithm Object Identifiers**

| Signature Algorithm | Object Identifier |
|---|---|
| RSA with SHA-1 and PKCS v1.5 padding | sha1WithRSAEncryption ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5} |
| RSA with SHA-256 and PKCS v1.5 padding | sha256WithRSAEncryption ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11} |
| RSA with SHA-256 and PSS padding | id-RSASSA-PSS ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 10} |
| ECDSA with SHA-256 | ecdsa-with-SHA256 ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 2} |
| ECDSA with SHA-384 | ecdsa-with-SHA384 ::= {iso(1) member-body(2) us(840) ansi-X9-62(10045) signatures(4) ecdsa-with-SHA2 (3) 3} |

### 3.2.2 Specification of Public Keys In X.509 Certificates

FIPS 201 requires generation and storage of an X.509 certificate to correspond with each asymmetric private key contained on the PIV Card. X.509 certificates include object identifiers to specify the cryptographic algorithm associated with a public key. Table 3-5, below, specifies the object identifiers that may be used in certificates to indicate the algorithm for a subject public key.

**Table 3-5. Public Key Object Identifiers for PIV Key Types**

| PIV Key Type | Asymmetric Algorithm | Object Identifier |
|---|---|---|
| PIV Authentication key;<br>Card Authentication key;<br>Digital Signature key | RSA | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} |
| | ECDSA | {iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1} |
| Key Management key | RSA | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} |
| | ECDH or ECC MQV | {iso(1) member-body(2) us(840) ansi-X9-62(10045) id-publicKeyType(2) 1} |

A single object identifier is specified in Table 3-5 for all elliptic curve keys. An additional object identifier must be supplied in a parameters field to indicate the elliptic curve associated with the key.[2] Table 3-6 identifies the named curves and associated OIDs. (RSA exponents are encoded with the modulus in the certificate's subject public key, so the OID is not affected.)

[2] Note that the parameters may be specified in the cardholder's public key certificate, or inherited from the issuer's certificate. Regardless of source, the OIDs specified in Table 3-5 apply.

**Table 3-6. ECC Parameter Object Identifiers for Approved Curves**

| Asymmetric Algorithm | Object Identifier |
|---|---|
| Curve P-256 | ansip256r1 ::= { iso(1) member-body(2) us(840) ansi-X9-62(10045) curves(3) prime(1) 7 } |
| Curve P-384 | ansip384r1 ::= { iso(1) identified-organization(3) certicom(132) curve(0) 34 } |

### 3.2.3 Specification of Message Digests in the SP 800-73 Security Object

SP 800-73 mandates inclusion of a Security Object consistent with the Authenticity/Integrity Code defined by the International Civil Aviation Organization (ICAO) in [MRTD]. This object contains message digests of other digital information stored on the card (e.g., the cryptographic keys and biometric information) and is digitally signed. Table 3-7 identifies the hash algorithms that may be used to compute the message digests. The set of acceptable algorithms depends upon the expiration date of the PIV Card, since the hash algorithm must protect the data during the entire card lifetime. The Security Object format identifies the hash algorithm used when computing the message digests by inclusion of an object identifier; the appropriate object identifiers are identified in Table 3-8.

**Table 3-7. Hash Algorithm Requirements for the 800-73 Security Object**

| Card Expiration Date | Algorithm |
|---|---|
| Through 12/31/2010 | SHA-1 or SHA-256 |
| After 12/31/2010 | SHA-256 or SHA-384 |

**Table 3-8. Hash Algorithm Object Identifiers for the 800-73 Security Object**

| Hash Algorithm | Algorithm OID |
|---|---|
| SHA-1 | id-sha1 ::= {iso(1) identified-organization(3) oiw(14) secsig(3) algorithms(2) 26} |
| SHA-256 | id-sha256 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 1} |
| SHA-384 | id-sha384 ::= {joint-iso-itu-t(2) country(16) us(840) organization(1) gov(101) csor(3) nistalgorithm(4) hashalgs(2) 2} |

# 4. Certificate Status Information

The FIPS 201 functional component *PIV Card Issuance and Management Subsystem* generates and distributes status information for PIV asymmetric keys. FIPS 201 mandates two formats for certificate status information:

- X.509 CRLs; *and*
- OCSP status response messages.

The CRLs and OCSP status responses are digitally signed to support authentication and integrity.

Table 4-1 below provides specific guidance for digital signatures on PIV status information. For signatures on the CRLs or OCSP status response messages, the size of the public key and the hash algorithm used to generate the signature may be determined by the date the CRL or OCSP message was generated.

**Table 4-1. Signature Algorithm and Key Size Requirements for PIV Status Information**

| CRL or OCSP Response Generation Date | Public Key Algorithms and Key Sizes | Hash Algorithms | Padding Scheme |
|---|---|---|---|
| Through 12/31/2010 | RSA (1024, 2048, or 3072 bits) | SHA-1 or SHA-256 | PKCS #1 v.1.5 |
| | RSA (1024, 2048, or 3072 bits) | SHA-256 | PSS |
| | ECDSA (Curve P-256) | SHA-256 | N/A |
| | ECDSA (Curve P-384) | SHA-384 | N/A |
| After 12/31/2010 | RSA (2048 or 3072 bits) | SHA-256 | PKCS #1 v.1.5, PSS |
| | ECDSA (Curve P-256) | SHA-256 | N/A |
| | ECDSA (Curve P-384) | SHA-384 | N/A |

CRLs and OCSP messages rely on object identifiers to specify which signature algorithm was used to generate the digital signature. The algorithms and key sizes specified in Table 3-3 must be used to sign CRLs and OCSP responses. The object identifiers specified in Table 3-4 must be used in CRLs and OCSP messages to identify the signature algorithm.

# 5. PIV Card Management Keys

PIV Cards may support card activation by the card management system to support card personalization and post-issuance card update. PIV Cards that support card personalization and post-issuance perform a challenge response protocol using a symmetric cryptographic key (i.e., the PIV Card Management Key) to authenticate the card management system. After successful authentication, the card management system can modify information stored the PIV Card. Table 5-1 below, establishes specific requirements for cryptographic algorithms and key sizes for PIV Card Management keys according to the card expiration date.

**Table 5-1. Algorithm and Key Size Requirements for Card Management Keys**

| Card Expiration Date | Algorithm |
|---|---|
| Through 12/31/2010 | 2TDEA<br>3TDEA<br>AES-128, AES-192, and AES-256 |
| After 12/31/2010 | 3TDEA<br>AES-128, AES-192, and AES-256 |

# 6. Identifiers for PIV Card Interfaces

SP 800-73 defines an application programming interface, the *End-Point Client-Application Programming Interface,* and a set of mandatory card commands, the *End-Point PIV Card Application Card Command Interface*. The command syntaxes for these interfaces identify PIV keys using one-byte key references; their associated algorithms are specified using on-byte algorithm identifiers. The same identifiers are used in both interfaces.

Section 6.1, below, specifies the key reference values for each of the PIV key types. Section 6.2 defines algorithm identifiers for each cryptographic algorithm supported by this specification. Section 6.3 identifies valid combinations of key reference values and algorithm identifiers based on the period of use.

## 6.1 Key Reference Values

A PIV Card key reference is a one-byte identifier that specifies a cryptographic key according to its PIV Key Type. Table 6-1 defines the key reference values used on the PIV interfaces.

**Table 6-1. Key References for PIV Key Types**

| PIV Key Type | Key Reference Value |
|---|---|
| PIV Authentication Key | '9A' |
| Card Management Key | '9B' |
| Digital Signature Key | '9C' |
| Key Management Key | '9D' |
| Card Authentication Key | '9E' |

## 6.2 PIV Card Algorithm Identifiers

A PIV Card algorithm identifier is a one-byte identifier that specifies a cryptographic algorithm and key size. For symmetric cryptographic operations, the algorithm identifier also specifies a mode of operation (i.e., CBC or ECB). Table 6-2 lists the algorithm identifiers for the cryptographic algorithms that may be recognized on the PIV interfaces. All other algorithm identifier values are reserved for future use.

**Table 6-2. Identifiers for Supported Cryptographic Algorithms**

| Algorithm Identifier | Algorithm – Mode |
|---|---|
| '00' | 3 Key Triple DES – ECB |
| '01' | 2 Key Triple DES – ECB |

| Algorithm Identifier | Algorithm – Mode |
|---|---|
| ‘02’ | 2 Key Triple DES – CBC |
| ‘03’ | 3 Key Triple DES – ECB |
| ‘04’ | 3 Key Triple DES – CBC |
| '06' | RSA |
| ‘07’ | RSA |
| ‘08’ | AES-128 – ECB |
| ‘09’ | AES-128 – CBC |
| ‘0A’ | AES-192 – ECB |
| ‘0B’ | AES-192 – CBC |
| ‘0C’ | AES-256 – ECB |
| ‘0D’ | AES-256 – CBC |
| ‘11’ | ECC: Curve P-256 |
| ‘14’ | ECC: Curve P-384 |

Note that both the ‘00’ and ‘03’ algorithm identifiers correspond to 3 Key Triple DES – ECB.

## 6.3 Algorithm Identifiers for PIV Key Types

Table 6-3 summarizes the set of algorithms supported for each key reference value based on the time period of use.

**Table 6-3. PIV Card Keys: Key References and Algorithms**

| PIV Key Type | Key Reference Value | Time Period for Use | Permitted Algorithm Identifiers |
|---|---|---|---|
| PIV Authentication Key | ‘9A’ | Through 12/31/2010 | ‘06’, ‘07’, ‘11’, ‘14’ |
| | | After 12/31/2010 | ‘07’, ‘11’, ‘14’ |
| Card Management Key | ‘9B’ | Through 12/31/2010 | ‘00’, ‘01’, ‘02’, ‘03’, ‘04’,’08’, 09’, ‘0A’, ‘0B’, ‘0C’, ‘0D’ |
| | | After 12/31/2010 | ‘00’, ‘03’, ‘04’,’08’, 09’, ‘0A’, ‘0B’, ‘0C’, ‘0D’ |
| Digital Signature Key | ‘9C’ | Through 12/31/2008 | ‘06’, ‘07’, ‘11’, ‘14’ |
| | | After 12/31/2008 | ‘07’, ‘11’, ‘14’ |
| Key Management Key | ‘9D’ | Through 12/31/2008 | ‘06’, ‘07’, ‘11’, ‘14’ |
| | | After 12/31/2008 | ‘07’, ‘11’, ‘14’ |
| Card Authentication Key | ‘9E’ | Through 12/31/2010 | ‘00’, ‘01’, ‘02’, ‘03’, ‘04’, ‘06’, ‘07’,’08’, 09’, ‘0A’, ‘0B’, ‘0C’, ‘0D’, ‘11’, ‘14’ |
| | | After 12/31/2010 | ‘00’, ‘03’, ‘04’, ‘07’,’08’, 09’, ‘0A’, ‘0B’, ‘0C’, ‘0D’, ‘11’, ‘14’ |

# Appendix A—Acronyms

The following abbreviations and acronyms are used in this standard:

| | |
|---|---|
| 2TDEA | Two key TDEA |
| 3TDEA | Three key TDEA |
| AES | Advanced Encryption Standard specified in [FIPS197]. |
| CA | Certificate Authority |
| CBEFF | Common Biometric Exchange Formats Framework |
| CHUID | Cardholder Unique Identifier |
| CRL | Certificate revocation list |
| ECDSA | Elliptic Curve Digital Signature Algorithm |
| ECDH | Elliptic Curve Diffie-Hellman Algorithm |
| ECC MQV | ECC Menezes-Qu-Vanstone Algorithm |
| FIPS | Federal Information Processing Standard |
| FISMA | Federal Information Security Management Act |
| ICAO | International Civil Aviation Organization |
| ITL | Information Technology Laboratory |
| MQV | Menezes-Qu-Vanstone cryptographic algorithm |
| NIST | National Institute of Standards and Technology |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| OMB | Office of Management and Budget |
| PIV | Personal Identity Verification |
| PKI | Public Key Infrastructure |
| PSS | Probabilistic Signature Scheme |
| RSA | Rivest, Shamir, Adleman cryptographic algorithm |
| SHA | Secure Hash Algorithm |
| SP | Special Publication |
| TDEA | Triple Data Encryption Algorithm; Triple DEA |

## Appendix B—References

[FIPS186-3] Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), (Revision of FIPS 186-2, June 2000), to be published. (See http://csrc.nist.gov)

[FIPS197] Federal Information Processing Standard 197, Advanced Encryption Standard (AES), November 2001. (See http://csrc.nist.gov)

[FIPS201-1] Federal Information Processing Standard 201-1, Personal Identity Verification (PIV) of Federal Employees and Contractors, March 2006. (See http://csrc.nist.gov)

[MRTD] PKI for Machine Readable Travel Documents Offering ICC Read-Only Access Version - 1.1 Date - October 01, 2004. Published by authority of the Secretary General, International Civil Aviation Organization.

[PKCS1] Jonsson, J., and B. Kaliski, "PKCS #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[RFC 3279] Polk, W., Housley, R., and L. Bassham, "Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation Lists (CRL) Profile", RFC 3279, April 2002.

[SP800-56A] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2006. (See http://csrc.nist.gov)

[SP800-57(1)] NIST Special Publication 800-57, Recommendation on Key Management – Part 1: General, May 2006. (See http://csrc.nist.gov)

[SP800-67] NIST Special Publication 800-67, Recommendation for Triple Data Encryption Algorithm Block Cipher, May 2004. (See http://csrc.nist.gov)

[SUITE B] NSA Fact Sheet: Suite B Cryptography. (See http://www.nsa.gov/ia/industry/crypto_suite_b.cfm)

[SP800-73-1] NIST Special Publication 800-73-1, Interfaces for Personal Identity Verification, March 2006. (See http://csrc.nist.gov)

[SP800-76] NIST Special Publication 800-76, Biometric Data Specification for Personal Identity Verification, February 2006. (See http://csrc.nist.gov)

## Appendix C—Errata

Special Publication 800-78-1 has been modified to enhance interoperability, simplify the development of relying party applications, and enhance alignment with the National Security Agency's *Suite B Cryptography*. [SUITE B] Revision 1 reduces the set of elliptic curves approved for use with PIV cards and the supporting infrastructure from six curves to two. The two curves recognized for use are Curve P-256 and Curve P-384, both of which are also specified in Suite B. Since the three smallest curves specified in 800-78 (P-224, B-233, and K-233) have been eliminated, SHA-224 is no longer required and has also been deleted. SHA-384 has been added for use with Curve P-384. Revision 1 also eliminates the largest size of RSA keys (3072 bits) on PIV cards.

These changes simplify applications that require maximum interoperability: the number of OIDs that must be recognized (e.g., in certificates) has been significantly reduced; and elliptic curve implementations of elliptic curve cryptography can be optimized for operations over two specific curves. This simplification is partially offset by the addition of SHA-384.

These changes also enhance support for protection of classified information. Suite B specifies that Elliptic Curve Public Key Cryptography using Curve P-256 and SHA-256 are appropriate for protecting classified information up to the SECRET level, while Curve P-384 and SHA-384 are necessary for the protection of TOP SECRET information. With appropriate testing, evaluation, and certification, PIV Cards supporting elliptic curve cryptography may also be certified as Suite B Products and used to protect classified information.

Specific changes to this document are as follows:

1. Cover page: Changed "800-78" to "800-78-1" and added "(Draft)" designation.
2. Cover page: Changed date from April 2005 to May 2006.
3. Throughout. Modified header to specify "Draft Special Publication 800-78-1".
4. Throughout. SP 800-56, 800-57, 800-73, and 800-76 have been completed or updated since initial publication. Textual references to "forthcoming" documents have been revised to reflect document completion. Citations in Appendix B - References have been updated as appropriate.
5. Page 2, Section 1.5: Added descriptions of Sections 6 and Appendix C to the Overview.
6. Page 3, section 2: To maximize interoperability, applications need to support the algorithms specified in Sections 3.2 *and* 3.3. While Section 3.2 limits the RSA keys on the PIV card 2048 bits, Section 3.3 supports 3072 bit RSA signatures on authentication information (e.g., certificates, CRLS, biometrics, and the CHUID). Section 3.3 also specifies hash algorithms and padding schemes for digital signatures.
7. Page 5: Deleted Curves P-224, K-233, B-233, K-283, and B-283 from the list of elliptic curves for PIV cards.
8. Page 5: Added Curve P-384.
9. Page 6, Table 3-1: Deleted 3072 bit RSA. Limited the set of elliptic curves to P-256 and P-384, consistent with the changes on page 5.
10. Page 6, Section 3.1. Corrected the lower bound for RSA exponent to specify 65,537.
11. Page 6, Table 3-2: Deleted row with exponent range for 3072 bit RSA.
12. Page 7, Section 3.2.1: Added a reference to FIPS 186.

13. Page 7, section 3.2.1: Interoperability warning to agencies specifies SHA-384 rather than SHA-224.
14. Page 7, Table 3.3: Text explicitly mandates use of SHA-256 with Curve P-256 and SHA-384 with CurveP-384 when generating signatures.
15. Page 8, Table 3-4: Added a new row specifying ECDSA with SHA-384. Deleted rows specifying ECDSA with SHA-1 and ECDSA with SHA-224.
16. Page 9, Table 3-6: Added row with the object identifier for Curve P-384. Deleted rows with object identifiers for Curves P-224, K-233, B-233, K-283, and B-283.
17. Page 9, Table 3-7: Deleted SHA-224 from the list of hash algorithms that may be used to compute the Security Object message digests on PIV cards that expire through 12/31/2010. Added SHA-384 to the list of hash algorithms that may be used to compute the Security Object message digests on PIV cards that expire after 12/31/2010.
18. Page 9, Table 3-8: Deleted the algorithm identifier for SHA-224; added the algorithm identifier for SHA-384.
19. Page 10, Table 4-1: Explicitly specified that Curve P-256 and SHA-256 may be used to sign CRLs and OCSP responses. Explicitly specified that Curve P-384 and SHA-384 may be used to sign CRLs and OCSP responses.
20. Page 10, Table 4-1: Deleted a general specification permitting use of EC curves with SHA-224 and SHA-256 to sign CRLs and OCSP responses.
21. Page 12: Added Section 6, Identifiers for PIV Card Interfaces.
22. Page 15, Appendix B: Added reference for Suite B.
23. Page 16: Added Appendix C, Errata.