NIST Special Publication 800-78-3
DRAFT

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

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

W. Timothy Polk
Donna F. Dodson
William E. Burr
Hildegard Ferraiolo
David Cooper

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

November 2010

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Dr. Patrick D. Gallagher, Deputy 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 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

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]. This document, Special Publication 800-78-3, 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 in 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 Publication 800-73, *Interfaces for Personal Identity Verification* [SP800-73], 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, key

establishment schemes, 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, *Application 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 Certification Authorities (CA) 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].
- 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.

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 *Card Holder 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. Certification Authorities (CA) 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 3.1 and 3.2.

FIPS 201 requires CAs and Online Certificate Status Protocol (OCSP) responders to generate and distribute digitally signed Certificate Revocation Lists (CRL) 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, 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 time periods with different sets of acceptable algorithms for each key type. Note that use of 1024-bit RSA for digital signature and key management keys was phased out in 2008. The use of 1024-bit RSA for authentication keys is permitted to leverage current products and promote efficient adoption of FIPS 201, but must be phased out by 12/31/2013. Two key Triple-DES (2TDEA) authentication keys must be phased out by 12/31/2010. These requirements anticipate 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 usually a random challenge (rather than sensitive information) and is generally not retained.

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]:

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

To promote interoperability, this specification further limits PIV Authentication and Card Authentication elliptic curve keys to a single curve (P-256). PIV cryptographic keys for digital signatures and key management may use P-256 or P-384, based on application requirements. There is no phase out date specified for either curve.

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 12/31/2013	RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	After 12/31/2013	RSA (2048 bits) ECDSA (Curve P-256)
Card Authentication Key	Through 12/31/2010	2TDEA 3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	1/1/2011 through 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (1024 or 2048 bits) ECDSA (Curve P-256)
	After 12/31/2013	3TDEA AES-128, AES-192, or AES-256 RSA (2048 bits) ECDSA (Curve P-256)
Digital Signature Key	After 12/31/2008	RSA (2048 bits) ECDSA (Curves P-256 or P-384)
Key Management Key	After 12/31/2008	RSA key transport (2048 bits); ECDH (Curves P-256 or 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 that is an odd positive integer greater than or equal to 65,537 and less than 2^{256}, as specified in Table 3-2.

Table 3-2. RSA Public Key Exponents

RSA Modulus Size	Minimum exponent	Maximum exponent
1024	65,537 ($2^{16} + 1$)	$2^{256} - 1$
2048	65,537	$2^{256} - 1$

This specification requires that the Key Management Key must be an RSA key transport key or an Elliptic Curve Diffie-Hellman (ECDH) key. The specifications for RSA key transport are [PKCS1] and [SP800-56B]; the specification for ECDH 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 PIV Card. FIPS 201 and SP 800-73 require digital signatures on the following objects stored on the PIV Card:

+ X.509 public key certificates;

- the CHUID;
- biometric information (e.g., fingerprints); and
- the SP 800-73 Security Object.

Approved Digital Signature algorithms are specified in [FIPS 186]. Table 3-3 provides specific requirements 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 X.509 public key certificates, the CHUID, Security Object, and stored biometrics, the hash algorithm that must be used to generate the signature is determined by the signature generation date. Agencies are cautioned that generating digital signatures with elliptic curve algorithms may initially limit interoperability.

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

Signature Generation Date[1]	Public Key Algorithms and Key Sizes	Hash Algorithms	Padding Scheme
Through 12/31/2010	RSA (2048 or 3072)	SHA-1	PKCS #1 v1.5
		SHA-256	PKCS #1 v1.5
		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)	SHA-256	PKCS #1 v1.5
		SHA-256	PSS
	ECDSA (Curve P-256)	SHA-256	N/A
	ECDSA (Curve P-384)	SHA-384	N/A

Note: 2010 is a transition period where both SHA-1 and SHA-256 are recommended for generation of RSA signatures. Beginning in 2011, only SHA-256 may be used to generate RSA signatures on PIV objects. RSA signatures generated with SHA-256 may use either the PKCS #1 v1.5 padding scheme or the Probabilistic Signature Scheme (PSS) padding as defined in [PKCS1]. (This specification does not permit generation of RSA signatures with SHA-1 and PSS padding, since most current implementations of RSA use the padding scheme defined in PKCS #1 v1.5). 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.

To determine signature generation dates for the purpose of PIV Data Model Testing as outlined in SP 800-85B, the following date attributes should be used:

- For each X.509 public key certificate: the notBefore time in the certificate.
- For all other objects:
  - the signingTime attribute (if present) in the object's Cryptographic Message Syntax (CMS), or
  - the notBefore time encoded in the PIV Authentication certificate if the signingTime attribute is omitted in the object's CMS.

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, below, must be used in FIPS 201 implementations to identify the signature algorithm.

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; Card Authentication Key; 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	{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. Table 3-6, below, 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.)

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 PIV Card and is digitally signed. This specification requires that the message digests of digital information be computed using the same hash algorithm used to generate the digital signature on the Security Object. The set of acceptable algorithms depends upon the signature generation date, as specified in Table 3-3. 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 3-7.

Table 3-7. Hash Algorithm Object Identifiers

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 using a key size and hash algorithm that satisfy the requirements for signing PIV information, as specified in Table 3-3[2], and that are at least as large as the key size and hash algorithm used to sign the certificate.

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

[2] CRLs and OCSP status responses that only provide status information for certificates that were signed with 1024-bit RSA keys may be signed using 1024-bit RSA keys. CRLs and OCSP status responses that only provide status information for certificates that were signed with RSA with SHA-1 and PKCS #1 v1.5 padding may be signed using RSA with SHA-1 and PKCS #1 v1.5 padding through 12/31/2013.

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 updates 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 in 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 3TDEA AES-128, AES-192, or AES-256
After 12/31/2010	3TDEA AES-128, AES-192, or AES-256

6. Identifiers for PIV Card Interfaces

SP 800-73 defines an application programming interface, the *End-Point PIV Client Application Programming Interface* (Part 3), and a set of mandatory card commands, the *End-Point PIV Card Application Card Command Interface* (Part 2). The command syntaxes for these interfaces identify PIV keys using one-byte key references; their associated algorithms are specified using one-byte algorithm identifiers. The same identifiers are used in both interfaces.

Section 6.1 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 for PIV Key Types.

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., 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
'03'	3 Key Triple DES – ECB
'06'	RSA 1024 bit modulus, $65,537 \leq \text{exponent} \leq 2^{864} - 1$
'07'	RSA 2048 bit modulus, $65,537 \leq \text{exponent} \leq 2^{1824} - 1$
'08'	AES-128 – ECB
'0A'	AES-192 – ECB
'0C'	AES-256 – ECB
'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 12/31/2013	'06', '07', '11'
		After 12/31/2013	'07', '11'
Card Management Key	'9B'	Through 12/31/2010	'00', '01', '03', '08', '0A', '0C'
		After 12/31/2010	'00', '03', '08', '0A', '0C'
Digital Signature Key	'9C'	After 12/31/2008	'07', '11', '14'
Key Management Key	'9D'	After 12/31/2008	'07', '11', '14'
Card Authentication Key	'9E'	Through 12/31/2010	'00', '01', '03', '06', '07', '08', '0A', '0C', '11'
		1/1/2011 Through 12/31/2013	'00', '03', '06', '07', '08', '0A', '0C', '11'
		After 12/31/2014	'00', '03', '07', '08', '0A', '0C', '11'

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	Certification Authority
CBEFF	Common Biometric Exchange Formats Framework
CHUID	Card Holder Unique Identifier
CRL	Certificate Revocation List
DES	Data Encryption Standard
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECDH	Elliptic Curve Diffie-Hellman
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
ICAO	International Civil Aviation Organization
ITL	Information Technology Laboratory
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] Federal Information Processing Standard 186-3, Digital Signature Standard (DSS), June 2009. (See http://csrc.nist.gov)

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

[FIPS201] Federal Information Processing Standard 201-1, Change Notice 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] Jakob Jonsson and Burt Kaliski, "PKCS #1: RSA Cryptography Specifications Version 2.1", RFC 3447, February 2003.

[SP800-56B] NIST Special Publication 800-56B, Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography, August 2009. (See http://csrc.nist.gov)

[SP800-56A] NIST Special Publication 800-56A, Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, March 2007. (See http://csrc.nist.gov)

[SP800-57(1)] NIST Special Publication 800-57, Recommendation for Key Management – Part 1: General, March 2007. (See http://csrc.nist.gov)

[SP800-73] NIST Special Publication 800-73-3, Interfaces for Personal Identity Verification, February 2010. (See http://csrc.nist.gov)

[SP800-76] NIST Special Publication 800-76-1, Biometric Data Specification for Personal Identity Verification, January 2007. (See http://csrc.nist.gov)