The attached DRAFT document (provided here for historical purposes) has been superseded by the following publication:

Publication Number: **NIST Special Publication (SP) 800-78-4**

Title: **Cryptographic Algorithms and Key Sizes for Personal Identity Verification**

Publication Date: **05/29/2015**

- Final Publication: https://doi.org/10.6028/NIST.SP.800-78-4 (which links to http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-4.pdf).
- Information on other NIST Computer Security Division publications and programs can be found at: http://csrc.nist.gov/

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

The following information was posted with the attached DRAFT document:

May 19, 2014

SP 800-78-4

DRAFT Cryptographic Algorithms and Key Sizes for Personal Identity Verification

NIST announces that Revised Draft Special Publication 800-78-4, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, is now available for public comment. The document has been modified to remove information about algorithms and key sizes that can no longer be used because their "Time Period for Use" is in the past. Revised Draft SP 800-78-4 also reflects changes to align with updates in Revised Draft SP 800-73-4. This document has been updated to reflect the disposition of comments that were received on the first draft of SP 800-78-4, which was published on May 13, 2013. The complete set of comments and dispositions is provided below (see last link for this draft below titled "Comments Received & Disposition from May 2013 draft to Revised Draft SP 800-78-4".

NIST requests comments on Revised Draft Special Publication 800-78-4 by 5:00pm EDT on ***June 16, 2014***. Please submit comments on Revised Draft SP 800-78-4 using the SP 800-78-4 comment template form (see third link below for Excel spreadsheet) to piv_comments @ nist.gov with "Comments on Revised Draft SP 800-78-4" in the subject line

Revised Draft NIST Special Publication 800-78-4

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

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

C O M P U T E R   S E C U R I T Y

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

Revised Draft NIST Special Publication 800-78-4

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

W. Timothy Polk
Donna F. Dodson
William E. Burr
Hildegard Ferraiolo
David Cooper
Computer Security Division
Information Technology Laboratory

May 2014

U.S. Department of Commerce
Penny Pritzker, Secretary

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

Authority

This publication has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347. NIST is responsible for developing information security standards and guidelines, including minimum requirements for Federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate Federal officials exercising policy authority over such systems. This guideline 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 Circular A-130, Appendix IV: *Analysis of Key Sections*. Supplemental information is provided in Circular A-130, Appendix III, *Security of Federal Automated Information Resources*.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on Federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other Federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-78
Natl. Inst. Stand. Technol. Spec. Publ. 800-78, 24 pages (May 2014)
http://dx.doi.org/10.6028/NIST.SP.XXX
CODEN: NSPUE2

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by Federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, Federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. All NIST Computer Security Division publications, other than the ones noted above, are available at http://csrc.nist.gov/publications.

Public comment period: *May 16, 2014* through *June 16, 2014*

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

Reports on Computer Systems Technology

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

Abstract

Federal Information Processing Standard 201 (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 Specifications for Personal Identity Verification* [SP800-76], that rely on cryptographic functions.

Keywords

cryptographic algorithm; FIPS 201; identity credential; Personal Identity Verification (PIV); smart cards

Acknowledgments

The authors wish to thank Sharon Keller from NIST, who contributed to the development of the Cryptographic Algorithm Validation Program validation requirements.

Trademark Information

Table of Contents

List of Tables

1 Introduction

Homeland Security Presidential Directive-12 (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 800-78-4, specifies the cryptographic algorithms and key sizes for PIV systems and is a companion document to FIPS 201.

1.1 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 Specifications for Personal Identity Verification* [SP800-76], that rely on cryptographic functions.

1.2 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 112 bits of security strength. For detailed guidance on the strength of cryptographic algorithms, see [SP800-57(1)], *Recommendation on Key Management – Part 1: General*.

1.3 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.

1.4 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 Application Administration 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 [SP800-73].
+ Section 7, *Cryptographic Algorithm Validation Testing Requirements*, specifies the cryptographic algorithm validation testing that must be performed on the PIV Card based on the keys and algorithms that it supports.
+ 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;
+ an asymmetric Card Authentication key;
+ a symmetric Card Authentication key;
+ an asymmetric digital signature key for signing documents and messages;
+ an asymmetric key management key, supporting key establishment or key transport, and up to twenty retired key management keys;
+ a symmetric PIV Card Application Administration Key; and
+ an asymmetric PIV Secure Messaging key, supporting the establishment of session keys for use with secure messaging.

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, except the PIV Secure Messaging key;
+ a secure messaging card verifiable certificate (CVC) for the PIV Secure Messaging key;
+ an Intermediate CVC for the public key needed to verify the signature on the secure messaging CVC;
+ 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 PIV Card Application Administration 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 six different classes of cryptographic keys to be used as credentials by the PIV cardholder:

+ the mandatory PIV Authentication key;
+ the mandatory asymmetric Card Authentication key;
+ an optional symmetric Card Authentication key;
+ a conditionally mandatory digital signature key;
+ a conditionally mandatory key management key;[1] and
+ an optional asymmetric key to establish session keys for secure messaging.

Table 3-1 establishes specific requirements for cryptographic algorithms and key sizes for each key type.

In addition to the key sizes, keys must be generated using secure parameters. Rivest, Shamir, Adleman (RSA) keys must be generated using a public exponent of 65,537. 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.

If the PIV Card Application supports the virtual contact interface [SP800-73] and the digital signature key, the key management key, or any of the retired key management keys are elliptic curve keys corresponding to Curve P-384, then the PIV Secure Messaging key shall use P-384, otherwise it may use P-256 or P-384.

[1] The digital signature and key management keys are mandatory if the cardholder has a government-issued email account at the time of credential issuance.

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

PIV Key Type	Algorithms and Key Sizes
PIV Authentication key	RSA (2048 bits) ECDSA (Curve P-256)
asymmetric Card Authentication key	RSA (2048 bits) ECDSA (Curve P-256)
symmetric Card Authentication key	3TDEA[2] AES-128, AES-192, or AES-256
digital signature key	RSA (2048 bits) ECDSA (Curve P-256 or P-384)
key management key	RSA key transport (2048 bits); ECDH (Curve P-256 or P-384)
PIV Secure Messaging key	ECDH (Curve P-256 or P-384)

While this specification requires that the RSA public exponent associated with PIV keys be 65,537, applications should be able to process RSA public keys that have any public exponent that is an odd positive integer greater than or equal to 65,537 and less than 2^{256}.

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 optional secure messaging card verifiable certificate (CVC);
+ the optional Intermediate CVC;
+ the CHUID;
+ biometric information (e.g., fingerprints); and
+ the SP 800-73 Security Object.

Approved digital signature algorithms are specified in [FIPS186]. Table 3-2 provides specific requirements for public key algorithms and key sizes, hash algorithms, and padding schemes for generating digital signatures for digitally signed information stored on the PIV Card. Agencies

[2] 3TDEA is Triple DES using Keying Option 1 from [SP800-67], which requires that all three keys be unique (i.e., $Key_1 \neq Key_2$, $Key_2 \neq Key_3$, and $Key_3 \neq Key_1$).

are cautioned that generating digital signatures with elliptic curve algorithms may initially limit interoperability.

Table 3-2. Signature Algorithm and Key Size Requirements for PIV Information

Public Key Algorithms and Key Sizes	Hash Algorithms	Padding Scheme
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: As of January 1, 2011, only SHA-256 may be used to generate RSA signatures on PIV objects. RSA signatures may use either the PKCS #1 v1.5 padding scheme or the Probabilistic Signature Scheme (PSS) padding as defined in [PKCS1]. The PSS padding scheme OID is independent of the hash algorithm; the hash algorithm is specified as a parameter (for details, see [PKCS1]).

The secure messaging CVC shall be signed using ECDSA (Curve P-256) with SHA-256 if it contains an ECDH (Curve P-256) subject public key, and shall be signed using ECDSA (Curve P-384) with SHA-384 otherwise. The Intermediate CVC shall be signed using RSA with SHA-256 and PKCS #1 v1.5 padding.

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 3-3, below, must be used in FIPS 201 implementations to identify the signature algorithm.[3]

Table 3-3. FIPS 201 Signature Algorithm Object Identifiers

Signature Algorithm	Object Identifier
RSA with SHA-1 and PKCS #1 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 #1 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, except the PIV Secure Messaging key. X.509 certificates include object identifiers to specify the cryptographic algorithm associated

[3] The OID for RSA with SHA-1 and PKCS #1 v1.5 padding is included in Table 3-3 since applications may encounter X.509 certificates and other data objects that were signed before January 1, 2011, using this algorithm.

with a public key. Table 3-4, below, specifies the object identifiers that may be used in certificates to indicate the algorithm for a subject public key.

Table 3-4. 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 3-4 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 3-5, 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 3-5. 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 is specified in Table 3-2. 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 3-6.[4]

Table 3-6. 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] The OID for SHA-1 is included in Table 3-6 since applications may encounter Security Objects that were signed before January 1, 2011, using RSA with SHA-1 and PKCS #1 v1.5 padding.

4 Certificate Status Information

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

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

The CRLs and OCSP status responses shall be 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 3-2, 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 3-3 must be used in CRLs and OCSP messages to identify the signature algorithm.

5 PIV Card Application Administration 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 Application Administration 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 Application Administration Keys.

Table 5-1. Algorithm and Key Size Requirements for PIV Card Application Administration Keys

Card Expiration Date	Algorithm
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 *PIV Client Application Programming Interface* (Part 3), and a set of mandatory card commands, the *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 (or suites of 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.

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 Secure Messaging key	'03'
retired key management key	'82', '83', '84', '85', '86', '87', '88', '89', '8A', '8B', '8C', '8D', '8E', '8F', '90', '91', '92', '93', '94', '95'
PIV Authentication key	'9A'
PIV Card Application Administration 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, or a suite of algorithms and key sizes. 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
'03'	3 Key Triple DES – ECB
'06'	RSA 1024 bit modulus, 65,537 $\leq$ exponent $\leq 2^{256} - 1$
'07'	RSA 2048 bit modulus, 65,537 $\leq$ exponent $\leq 2^{256} - 1$
'08'	AES-128 – ECB
'0A'	AES-192 – ECB
'0C'	AES-256 – ECB
'11'	ECC: Curve P-256
'14'	ECC: Curve P-384
'27'	Cipher Suite 2
'2E'	Cipher Suite 7

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

Algorithm identifiers '27' and '2E' represent suites of algorithms and key sizes for use with secure messaging and key establishment. Cipher Suite 2 (CS2) is the cipher suite used to establish session keys and for secure messaging when the PIV Secure Messaging key is an ECDH (Curve P-256) key, and Cipher Suite 7 (CS7) is the cipher suite used to establish session keys and for secure messaging when the PIV Secure Messaging key is an ECDH (Curve P-384) key. Details of secure messaging, the key establishment protocol, and the algorithms and key sizes for these two cipher suites are specified in SP 800-73, Part 2.

6.3 Algorithm Identifiers for PIV Key Types

Table 6-3 summarizes the set of algorithms supported for each key reference value.

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

PIV Key Type	Key Reference Value	Permitted Algorithm Identifiers
PIV Secure Messaging key	'03'	'27', '2E'
retired key management key	'82', '83', '84', '85', '86', '87', '88', '89', '8A', '8B', '8C', '8D', '8E', '8F', '90', '91', '92', '93', '94', '95'	'06', '07', '11', '14'
PIV Authentication key	'9A'	'07', '11'
PIV Card Application Administration Key	'9B'	'00', '03', '08', '0A', '0C'
digital signature key	'9C'	'07', '11', '14'
key management key	'9D'	'07', '11', '14'
asymmetric Card Authentication key	'9E'	'07', '11'
symmetric Card Authentication key	'9E'	'00', '03', '08', '0A', '0C'

7 Cryptographic Algorithm Validation Testing Requirements

As noted in Section 4.2.2 of [FIPS201], the PIV Card shall be validated under [FIPS140] with an overall validation of Level 2 and with Level 3 physical security. The scope of the Cryptographic Module Validation Program (CMVP) validation shall include all cryptographic operations performed over both the contact and contactless interfaces. Table 7-1 describes the Cryptographic Algorithm Validation Program (CAVP) tests that are required, at the time of publication, for each supported key and algorithm. If any changes are made to the CAVP validation requirements, the changes, along with the deadlines for conformance with these requirements, will be posted on NIST'S "Personal Identity Verification Program (NPIVP)" web page at http://csrc.nist.gov/groups/SNS/piv/npivp/index.html.

Table 7-1. Cryptographic Algorithm Validation Program (CAVP) Validation Requirements

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
PIV Authentication key	2048-bit RSA	*Key Generation and Signature Generation for 2048-bit RSA with public key exponent 65,537*	**Key Generation:** **186-2:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisite: RNG** or **DRBG; SHS** **186-4:** **186-4KEY(gen)**: FIPS186-4_Fixed_e, FIPS186-4_Fixed_e_Value PGM(Prime Generation Methods with supporting variables) **Prerequisites: RNG** or **DRBG; SHS** **Signature Generation:** **186-4 RSASP1 component:** (PKCS #1 v1.5 (SHA-256) and RSASSA-PSS)
	ECDSA (Curve P-256)	*Key Generation and Signature Generation for Curve P-256*	**Key Generation:** **186-2:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG** **Signature Generation:** **186-4 ECDSA Signature Generation component: CURVE(P-256 (SHA-256))** **Prerequisites: DRBG** or **RNG**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
asymmetric Card Authentication key	2048-bit RSA	*Signature Generation for 2048-bit RSA*	**Key Generation** (if key can be generated on card)**:** **186-2:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisite: RNG** or **DRBG; SHS** **186-4:** **186-4KEY(gen)**: FIPS186-4_Fixed_e, FIPS186-4_Fixed_e_Value PGM(Prime Generation Methods with supporting variables) **Prerequisites: RNG** or **DRBG; SHS** **Signature Generation:** **186-4 RSASP1 component:** (PKCS #1 v1.5 (SHA-256) and RSASSA-PSS)
	ECDSA (Curve P-256)	*Signature Generation for Curve P-256*	**Key Generation** (if key can be generated on card)**:** **186-2:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG** **Signature Generation:** **186-4 ECDSA Signature Generation component: CURVE(P-256 (SHA-256))** **Prerequisites: DRBG** or **RNG**
symmetric Card Authentication key	3TDEA	*Encryption and Decryption for 3TDEA*	**TECB**(e/d; KO 1)
	AES-128	*Encryption and Decryption for AES-128*	**ECB** (e/d; 128)
	AES-192	*Encryption and Decryption for AES-192*	**ECB** (e/d; 192)
	AES-256	*Encryption and Decryption for AES-256*	**ECB** (e/d; 256)

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
digital signature key	2048-bit RSA	*Key Generation and Signature Generation for 2048-bit RSA with public key exponent 65,537*	**Key Generation:** **186-2:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisite: RNG** or **DRBG; SHS** **186-4:** **186-4KEY(gen)**: FIPS186-4_Fixed_e, FIPS186-4_Fixed_e_Value PGM(Prime Generation Methods with supporting variables) **Prerequisites: RNG** or **DRBG; SHS** **Signature Generation:** **186-4 RSASP1 component:** (PKCS #1 v1.5 (SHA-256) and RSASSA-PSS)
	ECDSA (Curve P-256)	*Key Generation and Signature Generation for Curve P-256*	**Key Generation:** **186-2:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG** **Signature Generation:** **186-4 ECDSA Signature Generation component: CURVE(P-256 (SHA-256))** **Prerequisites: DRBG** or **RNG**
	ECDSA (Curve P-384)	*Key Generation and Signature Generation for Curve P-384*	**Key Generation:** **186-2:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG** **Signature Generation:** **186-4 ECDSA Signature Generation component: CURVE(P-384 (SHA-384))** **Prerequisites: DRBG** or **RNG**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
key management key	2048-bit RSA	*2048-bit RSA Key Transport*	**Key Generation** (if key can be generated on card)**:** **186-2:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisite: RNG** or **DRBG; SHS** **186-4:** **186-4KEY(gen)**: FIPS186-4_Fixed_e, FIPS186-4_Fixed_e_Value PGM(Prime Generation Methods with supporting variables) **Prerequisites: RNG** or **DRBG; SHS** **Key Transport:** **SP 800-56B RSADP component**
	ECDH (Curve P-256)	*Key Agreement for Curve P-256*	**Key Generation** (if key can be generated on card)**:** **186-2:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG** **Key Agreement:** **SP 800-56A Section 5.7.1.2 ECC CDH primitive component: CURVE(P-256)**
	ECDH (Curve P-384)	*Key Agreement for Curve P-384*	**Key Generation** (if key can be generated on card)**:** **186-2:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG** **Key Agreement:** **SP 800-56A Section 5.7.1.2 ECC CDH primitive component: CURVE(P-384)**
PIV Card Application Administration Key	3TDEA	*Encryption and Decryption for 3TDEA*	**TECB**(e/d; KO 1)
	AES-128	*Encryption and Decryption for AES-128*	**ECB** (e/d; 128)
	AES-192	*Encryption and Decryption for AES-192*	**ECB** (e/d; 192)
	AES-256	*Encryption and Decryption for AES-256*	**ECB** (e/d; 256)

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
PIV Secure Messaging key	Cipher Suite 2	*Key Generation for Curve P-256*	**Key Generation** (of card’s static ECDH key)**:** **186-2:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG**
		C(1e, 1s, ECC CDH) with Curve P-256	**ECC: SCHEME[OnePassDH (KC** <KARole: Responder > < KCRole: Provider > < KCType: Unilateral > < KDF: Concat >) (EC: P-256 (SHA256 CMAC_AES128)) **]** **Prerequisite: RNG** or **DRBG; SHS**
		CMAC with AES-128	**AES CMAC** (Generation/Verification) **(KS: 128;** Block Size(s): Full / Partial; **Msg Len(s)** Min: 32 Max: 12,745 ; Tag Length(s): 16)
		Encryption and Decryption for AES CBC 128	**AES CBC** (e/d; 128)
	Cipher Suite 7	*Key Generation for Curve P-384*	**Key Generation** (of card’s static ECDH key)**:** **186-2:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** or **RNG** **186-4:** **PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** or **RNG**
		C(1e, 1s, ECC CDH) with Curve P-384	**ECC: SCHEME[OnePassDH (KC** <KARole: Responder > < KCRole: Provider > < KCType: Unilateral > < KDF: Concat >) (ED: P-384 (SHA384 CMAC_AES256)) **]** **Prerequisite: RNG** or **DRBG; SHS**
		CMAC with AES-256	**AES CMAC** (Generation/Verification) **(KS: 256;** Block Size(s): Full / Partial; **Msg Len(s)** Min: 32 Max: 12,745 ; Tag Length(s): 16)
		Encryption and Decryption for AES CBC 256	**AES CBC** (e/d; 256)

Appendix A—Acronyms

The following abbreviations and acronyms are used in this standard:

3TDEA	Three key TDEA (TDEA with Keying Option 1 [SP800-67])
AES	Advanced Encryption Standard [FIPS197]
CA	Certification Authority
CAVP	Cryptographic Algorithm Validation Program
CBC	Cipher Block Chaining
CBEFF	Common Biometric Exchange Formats Framework
CDH	Cofactor Diffie-Hellman
CHUID	Card Holder Unique Identifier
CMAC	Cipher-Based Message Authentication Code
CMVP	Cryptographic Module Validation Program
CRL	Certificate Revocation List
CVC	Card Verifiable Certificate
DES	Data Encryption Standard
DRBG	Deterministic Random Bit Generator
ECB	Electronic Codebook
ECC	Elliptic Curve Cryptography
ECDH	Elliptic Curve Diffie-Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
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
PKCS	Public-Key Cryptography Standards
PKI	Public Key Infrastructure
PSS	Probabilistic Signature Scheme
RNG	Random Number Generator
RSA	Rivest, Shamir, Adleman cryptographic algorithm
SHA	Secure Hash Algorithm
SHS	Secure Hash Standard
SP	Special Publication
TDEA	Triple Data Encryption Algorithm; Triple DEA
TECB	TDEA Electronic Codebook

Appendix B—References

[FIPS140] Federal Information Processing Standard 140-2, *Security Requirements for Cryptographic Modules*, NIST, May 25, 2001. (See http://csrc.nist.gov)

[FIPS186] Federal Information Processing Standard 186-4, *Digital Signature Standard (DSS)*, July 2013. (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 201-2, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, August 2013. (See http://csrc.nist.gov)

[MRTD] ICAO Doc 9303, *Machine Readable Travel Documents, Part 3: Machine Readable Official Travel Documents, Volume 2: Specifications for Electronically Enabled MRtds with Biometric Identification Capability, 2008*. 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.

[SP800-67] NIST Special Publication 800-67 Revision 1, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, January 2012. (See http://csrc.nist.gov)

[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 Revision 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, May 2013. (See http://csrc.nist.gov)

[SP800-57(1)] NIST Special Publication 800-57, *Recommendation for Key Management – Part 1: General (Revision 3)*, July 2012. (See http://csrc.nist.gov)

[SP800-73] Revised Draft NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*. (See http://csrc.nist.gov)

[SP800-76] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013. (See http://csrc.nist.gov)