NIST Special Publication
NIST SP 800-78-5 ipd

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-78-5.ipd

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY
U.S. DEPARTMENT OF COMMERCE

NIST Special Publication
NIST SP 800-78-5 ipd

Cryptographic Algorithms and Key Sizes for Personal Identity Verification

Initial Public Draft

Hildegard Ferraiolo
Andrew Regenscheid
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-78-5.ipd

September 2023

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
Laurie E. Locascio, NIST Director and Under Secretary of Commerce for Standards and Technology

Authority

NIST Technical Series Policies

Publication History

Approved by the NIST Editorial Review Board on YYYY-MM-DD [Will be add in the final publication]
Supersedes NIST Series XXX (Month Year) DOI [Will be added in the final publication]

How to Cite this NIST Technical Series Publication:

Ferraiolo H, Regenscheid A (2023) Cryptographic Algorithms and Key Sizes for Personal Identity Verification. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-78-5 ipd. https://doi.org/10.6028/NIST.SP.800-78-5.ipd

Author ORCID iDs

Hildegard Ferraiolo: 0000-0002-7719-5999
Andrew Regenscheid: 0000-0002-3930-527X

Public Comment Period

September 27, 2023 – November 15, 2023

Submit Comments

piv_comments@nist.gov

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

All comments are subject to release under the Freedom of Information Act (FOIA).

Abstract

Federal Information Processing Standard 201-3 (FIPS 201-3) defines the requirements for Personal Identity Verification (PIV) life cycle activities, including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201-3 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 201-3, as well as the supporting infrastructure specified in FIPS 201-3 and the related NIST Special Publication (SP) 800-73, *Interfaces for Personal Identity Verification*, and NIST SP 800-76, *Biometric Specifications for Personal Identity Verification*, which rely on cryptographic functions.

Keywords

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

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.

Call for Patent Claims

This public review includes a call for information on essential patent claims (claims whose use would be required for compliance with the guidance or requirements in this Information Technology Laboratory (ITL) draft publication). Such guidance and/or requirements may be directly stated in this ITL Publication or by reference to another publication. This call also includes disclosure, where known, of the existence of pending U.S. or foreign patent applications relating to this ITL draft publication and of any relevant unexpired U.S. or foreign patents.

ITL may require from the patent holder, or a party authorized to make assurances on its behalf, in written or electronic form, either:

a) assurance in the form of a general disclaimer to the effect that such party does not hold and does not currently intend holding any essential patent claim(s); or

b) assurance that a license to such essential patent claim(s) will be made available to applicants desiring to utilize the license for the purpose of complying with the guidance or requirements in this ITL draft publication either:

   i. under reasonable terms and conditions that are demonstrably free of any unfair discrimination; or

   ii. without compensation and under reasonable terms and conditions that are demonstrably free of any unfair discrimination.

Such assurance shall indicate that the patent holder (or third party authorized to make assurances on its behalf) will include in any documents transferring ownership of patents subject to the assurance, provisions sufficient to ensure that the commitments in the assurance are binding on the transferee, and that the transferee will similarly include appropriate provisions in the event of future transfers with the goal of binding each successor-in-interest.

The assurance shall also indicate that it is intended to be binding on successors-in-interest regardless of whether such provisions are included in the relevant transfer documents.

Such statements should be addressed to: piv_comments@nist.gov

Table of Contents

List of Tables

Acknowledgments

Hildegard Ferraiolo and Andrew Regenscheid wish to thank their co-authors, David Cooper, W. Timothy Polk, Donna F. Dodson, and William E. Burr, who developed the earlier revisions of SP 800-78, as well as Sharon Keller from NIST, who contributed to the development of the Cryptographic Algorithm Validation Program validation requirements.

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, NIST Special Publication (SP) 800-78-5, specifies the cryptographic algorithms and key sizes for PIV systems and is a companion document to FIPS 201-3.

1.1. Purpose

FIPS 201-3 defines the requirements for PIV life cycle activities, including identity proofing, registration, PIV Card issuance, and PIV Card usage. FIPS 201-3 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 201-3, as well as the supporting infrastructure specified in FIPS 201-3 and the related NIST SP 800-73, *Interfaces for Personal Identity Verification* [SP800-73], and SP 800-76, *Biometric Specifications for Personal Identity Verification* [SP800-76], which 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. This 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.

1.3. Audience and Assumptions

This document is intended for 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 201-3*, identifies the cryptographic mechanisms and objects that employ cryptography as specified in FIPS 201-3 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 managing 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.
- The *References* section contains the list of documents used as references in this document.
- Appendix A, *Acronyms*, contains the list of acronyms used in this document.
- Appendix B, *Change Log*, describes the changes made to NIST SP 800-78 since its initial release.

2. Application of Cryptography in FIPS 201-3

FIPS 201-3 employs cryptographic mechanisms to authenticate cardholders, secure information stored on the PIV Card, and secure the supporting infrastructure. FIPS 201-3 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 201-3 and NIST SP 800-73 are:

- The asymmetric PIV Authentication key,
- An asymmetric Card Authentication key,
- A symmetric Card Authentication key (deprecated),
- An asymmetric digital signature key for signing documents and messages,
- An asymmetric key management key that supports key establishment or key transport and up to 20 retired key management keys,
- A symmetric PIV Card Application Administration Key, and
- An asymmetric PIV Secure Messaging key that supports the establishment of session keys for use with secure messaging and supporting cardholder authentication using the SM-AUTH authentication mechanism.

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 201-3, NIST SP 800-73, and NIST SP 800-76 include:

- The X.509 certificates for each asymmetric key on the PIV Card, except for 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 NIST 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 201-3 requires CAs and Online Certificate Status Protocol (OCSP) responders to generate and distribute digitally signed certificate revocation lists (CRL) and OCSP status messages, respectively. These certificate status 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 certificate status mechanisms specified in FIPS 201-3 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, which also describes rules for encoding the signatures to ensure interoperability.

FIPS 201-3 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 201-3 identifies a suite of objects that are stored on the PIV Card for use in authentication mechanisms or 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 201-3 and NIST SP 800-73 specify 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 (deprecated),
- 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 and to authenticate the cardholder using the SM-AUTH authentication mechanism.

All cryptographic algorithms employed shall provide at least 112 bits of security strength. Cryptographic keys that will remain in use after 2030 should provide 128 bits of security strength[2]. Federal departments and agencies should consider potential cryptographic key length migrations as part of their moderate-to-long term cryptographic transition and modernization plans, including the need to plan and invest for a future migration to post-quantum algorithms. Capital investments for PIV issuance and relying party systems should be selected with an emphasis on ensuring a timely migration to post-quantum algorithms once standards, technologies, and services are available. If a migration to longer cryptographic keys would require significant resources or infrastructure upgrades, federal departments and agencies may elect to defer these improvements until the post-quantum migration. Post-quantum algorithms will be specified in a future revision of this document once foundational standards supporting their use have been adopted.

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

[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.

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

Table 1. Algorithm and key size requirements for PIV key types

PIV Key Type	Algorithms and Key Sizes Through 2030	Algorithm and Key Sizes for 2031 and Beyond
PIV Authentication key	RSA (2048 or 3072 bits) ECDSA (Curve P-256 or P-384)	RSA 3072 bits ECDSA (Curve P-256 or P-384)
Asymmetric Card Authentication key	RSA (2048 or 3072 bits) ECDSA (Curve P-256 or P-384)	RSA 3072 bits ECDSA (Curve P-256 or P-384)
Symmetric Card Authentication key (deprecated)	3TDEA[3] (deprecated), AES-128, AES-192, or AES-256	AES-128, AES-192, or AES-256
Digital signature key	RSA (2048 or 3072 bits) ECDSA (Curve P-256 or P-384)	RSA 3072 bits ECDSA (Curve P-256 or P-384)
Key management key	RSA key transport (2048 or 3072 bits) ECDH (Curve P-256 or P-384)	RSA key transport 3072 ECDH (Curve P-256 or P-384)
PIV Secure Messaging key	ECDH (Curve P-256 or P-384)	ECDH (Curve P-256 or P-384)

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 65537. Elliptic curve keys must correspond to one of the following recommended curves from [FIPS186]:

- Curve P-256 or
- Curve P-384.

Note that elliptic curve keys are a faster option than RSA-based keys for the Card Authentication key for physical access since elliptic curve private key computation time is significantly shorter than RSA-based private key computation time. There is no phaseout 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 that correspond to Curve P-384, then the PIV Secure Messaging key shall use P-384. Otherwise, it may use P-256 or P-384.

While this specification requires that the RSA public exponent associated with PIV keys be 65537, 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 65537 and less than 2^{256}.

This specification requires the key management key to 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], and the specification for ECDH key is [SP800-56A].

[3] 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 $Key_3 \neq Key_1$).

3.2. Authentication Information Stored on the PIV Card

3.2.1. Specification of Digital Signatures on Authentication Information

FIPS 201-3 requires the use of digital signatures to protect the integrity and authenticity of information stored on the PIV Card. FIPS 201-3 and NIST 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 NIST SP 800-73-4 Security Object.

Approved digital signature algorithms are specified in [FIPS186]. **Table 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 are cautioned that generating digital signatures with elliptic curve algorithms may initially limit interoperability.

Table 2. Signature algorithm and key size requirements for PIV information

	Public Key Algorithms and Key Sizes	Hash Algorithms	Padding Scheme
Through 2030	RSA (2048, 3072 or 4096)	SHA-256 or SHA-384	PKCS #1 v1.5
		SHA-256 or SHA-384	PSS
	ECDSA (Curve P-256)	SHA-256	N/A
	ECDSA (Curve P-384)	SHA-384	N/A
2031 and Beyond	RSA (3072 or 4096)	SHA-256 or SHA-384	PKCS #1 v1.5
		SHA-256 or SHA-384	PSS
	ECDSA (Curve P-256)	SHA-256	N/A
	ECDSA (Curve P-384)	SHA-384	N/A

Note that 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 object identifier (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 201-3, NIST SP 800-73, and NIST SP 800-76 specify formats for the CHUID, the Security Object, the biometric information, and X.509 public key certificates, which rely on OIDs to specify which signature algorithm was used to generate the digital signature. The object identifiers specified in **Table 3** must be used in FIPS 201-3 implementations to identify the signature algorithm.[4,5]

Table 3. FIPS 201-3 signature algorithm object identifiers

Signature Algorithm	Object Identifier (OID)
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}
RSA with SHA-384 and PKCS #1 v1.5 padding	Sha384WithRSAEncryption ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
RSA with SHA-384 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 201-3 requires the generation and storage of an X.509 certificate to correspond with each asymmetric private key contained on the PIV Card, except for the PIV Secure Messaging key. X.509 certificates include object identifiers to specify the cryptographic algorithm associated with a public key. **Table 4** specifies the object identifiers that may be used in certificates to indicate the algorithm for a subject public key.

Table 4. Public key object identifiers for PIV key types

PIV Key Type	Asymmetric Algorithm	Object Identifier (OID)
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 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[6]. **Table 5** identifies the named curves and associated OIDs

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

[5] For the CHUID, Security Object, and biometric information, the signatureAlgorithm field of SignerInfo shall contain rsaEncryption (1.2.840.113549.1.1.1) when the signature algorithm is RSA with PKCS #1 v1.5 padding.

[6] RSA exponents are encoded with the modulus in the certificate's subject public key, so the OID is not affected.

Table 5. ECC parameter object identifiers for approved curves

Asymmetric Algorithm	Object Identifier (OID)
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 NIST SP 800-73-4 Security Object

NIST SP 800-73 mandates the 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 2**. The Security Object format identifies the hash algorithm used when computing the message digests by including an object identifier. The appropriate object identifiers are identified in **Table 6**.

Table 6. Hash algorithm object identifiers

Hash Algorithm	Object Identifier (OID)
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 201-3 functional component *PIV Card Issuance and Management Subsystem* generates and distributes status information for PIV asymmetric keys other than PIV Secure Messaging keys. FIPS 201-2 mandates two formats for certificate status information:

1. X.509 CRLs *and*
2. 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 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** 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 updates. 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 7** establishes specific requirements for cryptographic algorithms and key sizes for PIV Card Application Administration Keys.

Table 7. Algorithm and key size requirements for PIV Card application administration keys

Card Expiration Date	Algorithm
Through December 31, 2030	3TDEA (deprecated) AES-128, AES-192, or AES-256
After December 31, 2030	AES-128, AES-192, or AES-256

6. Identifiers for PIV Card Interfaces

NIST 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, and 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 8** defines the key reference values used on the PIV interfaces for PIV Key Types.

Table 8. Key references for PIV Key Types

PIV Key Type	Key Reference Value
PIV Secure Messaging key	'04'
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 9** 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 9. Identifiers for supported cryptographic algorithms

Algorithm Identifier	Algorithm – Mode
'00'	3 Key Triple DES – ECB (deprecated)
'03'	3 Key Triple DES – ECB (deprecated)
'05'	RSA 3072 bit modulus, 65537 ≤ exponent ≤ 2^{256} - 1
'06'	RSA 1024 bit modulus, 65537 ≤ exponent ≤ 2^{256} - 1
'07'	RSA 2048 bit modulus, 65537 ≤ exponent ≤ 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 3 Key Triple DES – ECB with identifier '00' and '03' is deprecated and will be removed in the next revision of this document.

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 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 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 NIST SP 800-73-4, Part 2.

6.3. Algorithm Identifiers for PIV Key Types

Table 10 summarizes the set of algorithms supported for each key reference value.

All cryptographic algorithms employed shall provide at least 112 bits of security strength. Cryptographic keys that will remain in use after 2030 should provide 128 bits of security strength[7]. Federal departments and agencies should consider potential cryptographic key length migrations as part of their moderate-to-long term cryptographic transition and modernization plans, including the need to plan and invest for a future migration to post-quantum algorithms. Capital investments for PIV issuance and relying party systems should be selected with an emphasis on ensuring a timely migration to post-quantum algorithms once standards, technologies, and services are available. If a migration to longer cryptographic keys would require significant resources or infrastructure upgrades, federal departments and agencies may elect to defer these improvements until the post-quantum migration. Post-quantum algorithms will be specified in a future revision of this document once foundational standards supporting their use have been adopted.

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

Table 10. PIV Card keys: Key references and algorithms

PIV Key Type	Key Reference Value	Algorithm Identifiers Through 2030	Algorithm Identifiers After 2030
PIV Secure Messaging key	'04'	'27', '2E'	'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'	'05', '06', '07', '11', '14'	'05', '06', '07', '11', '14'
PIV Authentication key	'9A'	'05','07', '11', '14'	'05', '11', '14'
PIV Card Application Administration Key	'9B'	'00', '03', '08', '0A', '0C'	'08', '0A', '0C'
Digital signature key	'9C'	'05', '07', '11', '14'	'05', '11', '14'
Key management key	'9D'	'05','07', '11', '14'	'05', '11', '14'
Asymmetric Card Authentication key	'9E'	'05','07', '11', '14'	'05', '11', '14'
Symmetric Card Authentication key (deprecated)	'9E'	'00', '03', '08', '0A', '0C'	'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 11**[8] describes the Cryptographic Algorithm Validation Program (CAVP) tests that are required for each supported key and algorithm at the time of publication[9]. If any changes are made to the CAVP validation requirements, the changes and 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.

[8] Terms used in this section are from the corresponding algorithm validation list available at http://csrc.nist.gov/groups/STM/cavp/validation.html.
[9] TDEA has been removed from **Table 11** since [SP 800-131A Revision 2] has deprecated its use through 2023 and disallowed its use after 2023. Consequently, on January 1, 2024, CMVP will move validated TDEA implementations to the FIPS 140-mode non-approved historical validation list.

Table 11. 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 65537*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Signature Generation:** **RSASP1 component:** (Mod2048)
	3072-bit RSA	*Key Generation and Signature Generation for 3072-bit RSA with public key exponent 65537*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 3072 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen)**: FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Signature Generation:** **RSASP1 component:** (Mod3072)
	ECDSA (Curve P-256)	*Key Generation and Signature Generation for Curve P-256*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** **Signature Generation:** **ECDSA Signature Generation component:** **CURVE(P-256 tested with input length 256 bits)** **Prerequisites: DRBG**
	ECDSA (Curve P-384)	*Key Generation and Signature Generation for Curve P-384*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
			Signature Generation: **ECDSA Signature Generation component:** **CURVE(P-384 tested with input length 384 bits)** **Prerequisites: DRBG**
Asymmetric Card Authentication key	2048-bit RSA	*Signature Generation for 2048-bit RSA*	**Key Generation** (if key can be generated on card)**:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Signature Generation:** **RSASP1 component:** (Mod2048)
	3072-bit RSA	*Signature Generation for 3072-bit RSA*	**Key Generation** (if key can be generated on card)**:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 3072 PubKey Values: 65537) **Prerequisite: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Signature Generation:** **RSASP1 component:** (Mod3072)
	ECDSA (Curve P-256)	*Signature Generation for Curve P-256*	**Key Generation** (if key can be generated on card)**:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** **Signature Generation:** **ECDSA Signature Generation component:** **CURVE(P-256 tested with input length 256 bits)** **Prerequisites: DRBG**
	ECDSA (Curve P-384)	*Signature Generation for Curve P-384*	**Key Generation** (if key can be generated on card)**:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** **186-4:**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
			PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits and/or **TestingCandidates))** **Prerequisites: DRBG** **Signature Generation:** **ECDSA Signature Generation component:** **CURVE(P-384 tested with input length 384 bits)** **Prerequisites: DRBG**
Symmetric Card Authentication key	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)
Digital signature key	2048-bit RSA	*Key Generation and Signature Generation for 2048-bit RSA with public key exponent 65537*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Signature Generation:** **RSASP1 component:** (Mod2048)
	3072-bit RSA	*Key Generation and Signature Generation for 3072-bit RSA with public key exponent 65537*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 3072 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Signature Generation:** **RSASP1 component:** (Mod3072)
	ECDSA (Curve P-256)	*Key Generation and Signature Generation for Curve P-256*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
			Prerequisites: DRBG **Signature Generation:** **ECDSA Signature Generation component:** **CURVE(P-256 tested with input length 256 bits)** **Prerequisites: DRBG**
	ECDSA (Curve P-384)	*Key Generation and Signature Generation for Curve P-384*	**Key Generation:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** **Signature Generation:** **ECDSA Signature Generation component:** **CURVE(P-384 tested with input length 384 bits)** **Prerequisites: DRBG**
Key management key	2048-bit RSA	*2048-bit RSA Key Transport*	**Key Generation** (if key can be generated on card)**:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 2048 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: DRBG; SHS** **Key Transport:** **SP 800-56B RSADP component**
	3072-bit RSA	*3072-bit RSA Key Transport*	**Key Generation** (if key can be generated on card)**:** **186-2** (for revalidation scenarios only)**:** **Key**(gen)(MOD: 3072 PubKey Values: 65537) **Prerequisites: DRBG; SHS** **186-4:** **186-4KEY(gen):** FIPS186-4_Fixed_e (65537) or FIPS186-4_Random_e PGM(Prime Generation Methods) **Prerequisites: 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** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
			Key Agreement: **SP 800-56A-3 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** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG** **Key Agreement:** **SP 800-56A-3 Section 5.7.1.2 ECC CDH primitive component: CURVE(P-384)**
PIV Card Application Administration Key	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)
PIV Secure Messaging key	Cipher Suite 2	*Key Generation for Curve P-256*	**Key Generation** (of card's static ECDH key)**:** **186-2** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-256)** **Prerequisites: DRBG** **186-4:** **PKG (Public Key Generation): CURVE(P-256 (ExtraRandomBits** and/or **TestingCandidates))** **Prerequisites: DRBG**
		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)) **]** **Prerequisites: DRBG; SHS**
		CMAC with AES-128	**AES CMAC** (Generation/Verification) **(KS: 128; 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** (for revalidation scenarios only)**:** **PKG (Public Key Generation): CURVE(P-384)** **Prerequisites: DRBG** **186-4:**

Supported Private Keys	Supported Algorithm	Required Functionality	Minimum CAVP Validation Requirements
			PKG (Public Key Generation): CURVE(P-384 (ExtraRandomBits and/or **TestingCandidates)) Prerequisites: DRBG**
		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)) **]** **Prerequisites: DRBG; SHS**
		CMAC with AES-256	**AES CMAC** (Generation/Verification) **(KS: 256; Msg Len(s)** Min: 32 Max: 12 745 ; Tag Length(s): 16)
		Encryption and Decryption for AES CBC 256	**AES CBC** (e/d; 256)

References

[FIPS140] Federal Information Processing Standard 140-3, *Security Requirements for Cryptographic Modules*, March 22, 2019. https://doi.org/10.6028/NIST.FIPS.140-3

[FIPS186] Federal Information Processing Standard 186-4, *Digital Signature Standard (DSS)*, July 2013. https://doi.org/10.6028/NIST.FIPS.186-4

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

[FIPS201] Federal Information Processing Standard 201-3, *Personal Identity Verification (PIV) of Federal Employees and Contractors*, January 2022. https://doi.org/10.6028/NIST.FIPS.201-3

[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,* 3rd edition, International Civil Aviation Organization: Montreal, Quebec, Canada, 2008. https://www.icao.int/publications/pages/publication.aspx?docnum=9303

[PKCS1] Moriarty K (ed.), Kaliski B, Jonsson J, Rusch A, *PKCS #1: RSA Cryptography Specifications Version 2.2*, RFC 8017, November 2016. https://doi.org/10.17487/RFC8017

[SP800-56A] NIST Special Publication 800-56A Revision 3, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, April 2018. https://doi.org/10.6028/NIST.SP.800-56Ar3

[SP800-56B] NIST Special Publication 800-56B Revision 2, *Recommendation for Pair-Wise Key-Establishment Schemes Using Integer Factorization Cryptography*, March 2019. https://doi.org/10.6028/NIST.SP.800-56Br2

[SP800-57(1)] NIST Special Publication 800-57*, Recommendation for Key Management – Part 1: General (Revision 5)*, May 2020. https://csrc.nist.gov/publications/

[SP800-67] NIST Special Publication 800-67 Revision 2, *Recommendation for the Triple Data Encryption Algorithm (TDEA) Block Cipher*, November 2017. https://doi.org/10.6028/NIST.SP.800-67r2

[SP800-73] NIST Special Publication 800-73-4, *Interfaces for Personal Identity Verification*, May 2015. https://doi.org/10.6028/NIST.SP.800-73-4

[SP800-76] NIST Special Publication 800-76-2, *Biometric Specifications for Personal Identity Verification*, July 2013. https://doi.org/10.6028/NIST.SP.800-76-2

[SP800-131A] NIST Special Publication 800-131A Revision 2, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, March 2019. https://doi.org/10.6028/NIST.SP.800-131Ar2

Appendix A. List of Symbols, Abbreviations, and 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]

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

RSA
Rivest-Shamir-Adleman Cryptographic Algorithm

SHA
Secure Hash Algorithm

SHS
Secure Hash Standard

SP
Special Publication

TDEA
Triple Data Encryption Algorithm; Triple DEA

Appendix B. Change Log

This appendix is informative and provides an overview of the changes made to NIST SP 800-78 since its initial release.

In August 2007, Revision 1 enhanced alignment with the National Security Agency's Suite B Cryptography by:

- Reducing the set of elliptic curves approved for use with PIV cards from six curves to two,
- Adding SHA-384 with Curve P-384, and
- Eliminating the largest size of RSA keys (3072 bits) on PIV cards.

In February 2010, Revision 2 updates included:

- Realigning with the NSA Suite B Cryptographic specification by removing discontinued Elliptic Curve MQV as a key agreement scheme,
- Aligning with FIPS 186-3 by removing RSA 4096 as an algorithm and key size for generating signatures for PIV data objects, and
- Eliminating the redundant cipher block chaining (CBC) mode of encryption for symmetric authentication purposes (challenge and response)

In December 2010, Revision 3 updates included:

- Aligning the set of acceptable RSA public key exponents with FIPS 186-3 and
- Extending the permitted use of SHA-1 after December 31, 2010, when signing revocation information under limited circumstances.

In 2014, Revision 4 updates included:

- Adding algorithm and key size requirements for secure messaging,
- Adding Cryptographic Algorithm Validation Program (CAVP) validation testing requirements, and
- Clarifying that RSA public keys may only have a public exponent of 65537.

In 2023, Revision 5 updates incorporate the following changes:

- **Table 1** reflects additional higher strength keys with at least 128-bit security and suggested sunsets of lower sized keys by 2030 in anticipation of the recommended migration to 128-bit security strength in 2031.
- Accommodation of the Secure Messaging Authentication key
- Deprecation of the symmetric card authentication key
- Deprecation of 3TDEA algorithm with identifiers '00' and '03'
- Removal of the retired RNG from CAVP PIV component testing where applicable