وزارة المواصلات والاتصالات
MINISTRY OF TRANSPORT AND COMMUNICATIONS

Electronic Signature Algorithms Standard

Version: 1.0

Author: Qatar Public Key Infrastructure Section

Document Classification: PUBLIC

Published Date: June 2018

Document Information

Date	Version	Reviewed By
04/06/2018	1.0	Qatar National PKI Team

Content

1. Overview

This document represents the rest of the previous document "**Electronic Signature: Overview & Specification**". The present document provides requirements on selection of cryptographic suites with particular emphasis on interoperability. The present document lists cryptographic suites used for the creation and validation of electronic signature. All requirement listed in this document shall be applied as a national standard.

2. Introduction

1. Objective of the document

In order to ensure an adequate degree of cryptographic security for the generation and verification of electronic signatures, several organizations have recommended the use of certain hashing and electronic signature algorithms: **NIST**, **ANSSI**, **Ecrypt II**, **and BSI**.

The objectives of this document are to present:

- The security properties of an electronic signature.
- The recommended algorithms for the hash functions, the robustness and the lifetime of these algorithms.
- The recommended algorithms for the electronic signature and the lifetime of the key sizes used by these algorithms.

2. Audience

This document is intended for developers of electronic signature applications as well as anyone else who needs to deploy the electronic signature.

3. Security properties of electronic signature

Computer security has several purposes. In particular, the electronic signature ensures the following objectives:

- **Authentication**: consists in ensuring the identity of a user, which is to say to guarantee to each of the correspondents that his partner is the one he thinks he is.
- **Integrity**: Verifying the integrity of the data consists of determining whether the data has not been altered during the communication (accidentally or intentionally).
- **Non-repudiation**: guarantee that none of the correspondents can deny the transaction.

4. Hash algorithms

1. Hash functions

A hash function **H** is a function which, from a message **x** of any size, computes a bit string **H (x)** of fixed size called fingerprint (or hash, or condensed). A hash function is a mathematical function that controls the integrity of a message.

2. Hash function properties

A hash function h must verify the following three properties:

- **Collision resistance**: It is computationally infeasible to find two different inputs to the hash function that have the same hash value. That is, if **H** is a hash function, it is computationally infeasible to find two different inputs **x** and **x'** for which **H (x) = H (x')**.
- **Preimage resistance**: Given a randomly chosen hash value, **H_value**, it is computationally infeasible to find an **x** so that **H (x)** = **H_value**. This property is also called the one-way property.
- **Second preimage resistance**: It is computationally infeasible to find a second input that has the same hash value as any other specified input. That is, given an input **x**, it is computationally infeasible to find a second input **x'** that is different from x, such that **H (x) = H (x')**.

3. Approved Hash Algorithms

Currently, there are seven approved hash algorithms specified in **FIPS 180-4**: **SHA-1**, **SHA-224**, **SHA-256**, **SHA-384**, **SHA-512**, **SHA-512/224** and **SHA-512/256**. These hash algorithms produce outputs of **160**, **224**, **256**, **384**, **512**, **224** and **256** bits, respectively. The output of a hash algorithm is commonly known as a message digest, a hash value or a hash output.

4. Recommendations

The list of hash functions in table 1 **shall** be used. The functions shall be implemented as per the reference listed in table 1 and shall follow the recommendations provided in the SOG-IS Agreed Cryptographic Mechanisms.

Short hash function name	References
SHA-256	FIPS Publication 180-4 [1]
SHA-384	FIPS Publication 180-4 [1]
SHA-512	FIPS Publication 180-4 [1]
SHA-512/256	FIPS Publication 180-4 [1]
SHA3-256	FIPS Publication 202 [16]
SHA3-384	FIPS Publication 202 [16]
SHA3-512	FIPS Publication 202 [16]

Table 1**: CSP-PMA agreed Hash Functions**

5. Strengths of the Approved Hash Algorithms

Table 2 provides a summary of the security strengths for the hash function security properties (discussed in the previous section) of the approved hash functions.

	SHA256	SHA384	SHA512	SHA512/224	SHA512/256
Collision Resistance Strength in bits	128	192	256	112	128
Preimage Resistance Strength in bits	256	384	512	224	256
Second Preimage Resistance Strength in bits	201- 256	384	394- 512	224	256

Table 2: **Strengths of the Security Properties of the Approved Hash Algorithms**

The latest cryptanalytic results for **SHA-1** [**SHA1 Attack**] indicate that it may have a collision resistance strength that is considerably less than its expected strength of 80 bits. Based on security and performance reasons, **sha1** and **sha-224** should not be used.

The expected preimage resistance strengths of the approved hash functions are provided in the above table. At the time that this Recommendation was written, there had been no known short cuts for finding preimages of the hash values generated by the approved hash algorithms.

Except for **SHA-384**, **SHA-512/224** and **SHA-512/256**, the second preimage resistance strengths of the approved hash functions depend not only on the functions themselves, but also on the sizes of the messages that the hash functions process [Second Preimage Attack]. In Table 2, the low end of each range applies to the situation where the length of the message input to the hash function is the maximum length allowed by the hash function, while the high end of the range applies to the situation where the message input length is relatively small. In the case of **SHA-384**, **SHA-512/224** or **SHA-512/256**, the second preimage resistance strength does not depend on the message length.

Note that the preimage resistance and the second preimage resistance strengths are greater than the collision resistance strength for each of the approved hash algorithms specified in **FIPS 180-4**.

6. Lifetime of hash algorithms

The lifetime of the hash algorithms is highly dependent on the size of the message digest. The following table's presents the message digest sizes accepted for the years based on the recommendations of the ECRYPT II, NIST, ANSSI and BSI organizations.

Hash Algorithms	ECRYPT II (2012)	NIST (2016)	ANSSI (2014)	BSI (2017)
SHA-224	• 2018-2020 • 2020-2030	• 2016-2030	• 2014-2020	
SHA-256	• 2018-2040	• 2016-2030 & Beyond	• 2021-2030 • > 2030	• 2017-2022 • > 2022
SHA-384		• 2016-2030 & Beyond		• 2017-2022 • > 2022
SHA-512				• 2017-2022 • > 2022
SHA-512/224	• 2018-2020 • 2020-2030	• 2016-2030	• 2014-2020	
SHA-512/256	• 2018-2040	• 2016-2030 & Beyond	• 2021-2030 • > 2030	• 2017-2022 • > 2022
SHA3-224	• 2018-2020 • 2018-2030	• 2016-2030	• 2014-2020	
SHA3-256	• 2018-2040	• 2016-2030 & Beyond	• 2021-2030 • > 2030	• 2017-2022 • > 2022
SHA3-384		• 2016-2030 & Beyond		• 2017-2022 • > 2022
SHA3-512				• 2017-2022 • > 2022

Table 3: **Organization's Recommendation**

CSP-PMA agree the use of one of hash functions listed on table 4. The list of hash functions in table 4 **shall** be used. The hash functions listed in table 4 are expected to remain suitable during X years.

Entry name of the hash function	1 year (2018)	3 years (2020)	6 years (2023)
SHA-256	usable	usable	Usable
SHA-384	usable	usable	Usable
SHA-512	usable	usable	Usable
SHA3-256	usable	usable	Usable
SHA3-384	usable	usable	Usable
SHA3-512	usable	usable	Usable

Table 4**: CSP-PMA Recommendation: Hash functions for a resistance during X years**

5. Electronic signature Algorithms

1. General discussion

A digital signature is an electronic analogue of a written signature; the digital signature can be used to provide assurance that the claimed signatory signed the information. In addition, a digital signature may be used to detect whether or not the information was modified after it was signed (i.e., to detect the integrity of the signed data). These assurances may be obtained whether the data was received in a transmission or retrieved from storage.

The **Electronic Commerce and Transactions Law** No. (**16**) Of **2010** define the electronic signature as "letters, numbers, symbols or others affixed to a data message, which uniquely identify the signatory from others in order to indicate the signatory's approval on the data message".

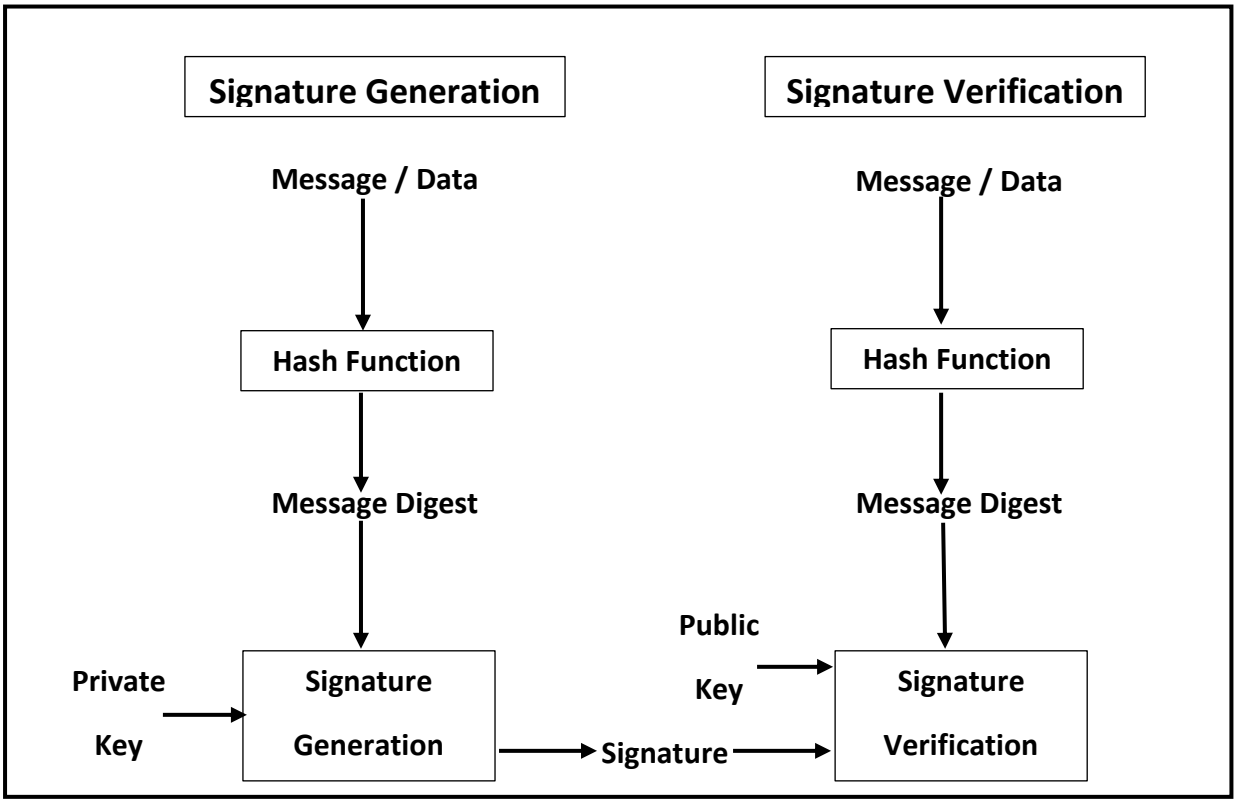

Figure 1: **Digital Signature Processes**

A digital signature algorithm includes a signature generation process and a signature verification process. A signatory uses the generation process to generate a digital signature on data; a verifier uses the verification process to verify the authenticity of the signature. Each signatory has a public and private key and is the owner of that key pair. As shown in **Figure 1**, the private key is used in the signature generation process. The key pair owner is the only entity that is authorized to use the private key to generate digital signatures. In order to prevent other entities from claiming to be the key pair owner and using the private key to generate fraudulent signatures, the private key must remain secret. The approved digital signature algorithms are designed to prevent an adversary who does not know the signatory's private key from generating the same signature as the signatory on a different message.

A properly implemented digital signature algorithm that meets the requirements of this document can provide these services.

2. Electronic Signature Algorithms Recommendations

The list of signature algorithms given in table 5 **shall** be used. The algorithms shall be implemented as per the reference listed in table 5 and shall follow the recommendations provided in the SOG-IS Agreed Cryptographic Mechanisms.

Short signature algorithm name	References
RSA-PKCS#1v1_5	IETF RFC 3447
RSA-PSS	IETF RFC 3447
DSA (FF-DLOG DSA)	FIPS Publication 186-4 ISO/IEC 14888-3
EC-DSA (EC-DLOG EC-DSA)	FIPS Publication 186-4
EC-SDSA-opt	ISO/IEC 14888-3

Table 5: **CSP-PMA agreed Digital Signature Algorithms**

2.1. DSA signature algorithm

The DSA signature algorithm is defined in the [**FIPS 186-4**] standard for the following key sizes: **1024**, **2048**, and **3072** bits. The **DSA** produces electronic signatures of **320**, **448** and **512** bits. The dissemination of **DSA** in trust services is low. Therefore, it is suggested to use other more widely deployed algorithms unless it is the only alternative for interoperability.

2.1.1. Recommendation

The parameters defined in following tables should be used.

	1 year (2018)	3 years (2020)	6 years (2023)
Key Size	2048	2048	3072

Table 6: **Recommended parameters for DSA**

2.2. RSA signature algorithm

RSA is an asymmetric cryptographic algorithm. This algorithm has been specified in standards [**ANSI X9.31**] and [**PKCS 1**] and has been adopted for the calculation of electronic signatures in the standard [**FIPS 186-4**].

2.2.1. Recommendation

The parameters defined in following tables should be used.

	1 year (2018)	3 years (2020)	6 years (2023)
Key Size	≥ 1900	≥ 1900	≥ 3000

Table 7: **Recommended parameters for RSA**

2.3. ECDSA signature algorithm

ECDSA is a public key cryptosystem based on elliptic curves for computing the electronic signature. This algorithm is defined in the [**ANSI X9.62**] standard and the guidelines for its implementation are given in the [**FIPS 186-4**] standard. **ECDSA** produces electronic signatures with a size equal to twice the length of the key size.

2.3.1. Recommendation

The parameters defined in following tables should be used.

	1 year (2018)	**3 years (2020)**	**6 years (2023)**
Key Size	256, 384 or 512	256, 384 or 512	256, 384 or 512

Table 8: **Recommended parameters for ECDSA**

6. Electronic Signatures Suites

1. Signature Suites

Table 9 reflects the combination of the **CSP-PMA** recommended hash functions and signature algorithms. The signature suites listed in table 9 **shall** be used.

Entry name of the signature suite	**Entry name for the hash function**	**Entry name for the signature algorithm**
sha256-with-rsa	SHA-256	RSA-PKCSv1_5
sha512-with-rsa	SHA-512	RSA-PKCSv1_5
rsa-pss with mgf1SHA-256Identifier	SHA-256	RSA-PSS
rsa-pss with mgf1SHA-512Identifier	SHA-512	RSA-PSS
rsa-pss with mgf1SHA3-Identifier	SHA3-256, SHA3-384 or SHA3-512	RSA-PSS
sha224-with-ecdsa	SHA-224	EC-DSA
sha2-with-ecdsa	SHA-256, SHA-384 or SHA-512	EC-DSA
sha2-with-ecsdsa	SHA-256, SHA-384 or SHA-512	EC-SDSA-opt
sha3-with-ecdsa	SHA3-256, SHA3- 384 or SHA3-512	EC-DSA
sha3-with-ecsdsa	SHA3-256, SHA3- 384 or SHA3-512	EC-SDSA-opt

Table 9: **Signature Suites**

2. Recommendations

Table 10 summarizes the recommendations from all tables above. The following table provides **CSP-PMA**'s requirements on hash functions, and (digital) signature suites to be used with the data structures used in the context of digital signatures remain suitable during X years. The list of signature suites given in table 13 **shall** be used (The parameters defined in following tables should be used).

Entry name of the signature suite	1 year (2018)	3 years (2020)	6 years (2023)
sha256-with-rsa	≥ 1 900	≥ 1 900	not recommended
sha512-with-rsa	≥ 1 900	≥ 1 900	not recommended
rsa-pss with mgf1SHA-256Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA-512Identifier	≥ 1 900	≥ 1 900	≥ 3 000
rsa-pss with mgf1SHA3-Identifier	≥ 1 900	≥ 1 900	≥ 3 000
sha256-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha512-with-dsa	2 048	2 048	3 072
sha224-with-ecdsa	legacy		
sha2-with-ecdsa	recommended		
sha2-with-ecsdsa	recommended		
sha3-with-ecdsa	recommended		
sha3-with-ecsdsa	recommended		

Table 10: **CSP-PMA recommended key sizes versus time for signature suites**

References

- **[ETSI TS 119 312]** TS 119 312; Electronic Signatures and Infrastructures (ESI); Cryptographic Suites, May 2017
- [**SOG-IS Crypto Evaluation Scheme**] SOG-IS Crypto Working Group; Agreed Cryptographic Mechanisms, May 2016.
- [**BSI Technical Guideline**] BSI TR-02102-1; Cryptographic Mechanisms: Recommendations and Key Lengths, January 2018
- [**FIPS PUB 186-4**] FIPS 186-4; Digital Signature Standard (DSS), July 2013
- [**NIST Special Publication 800-107**] SP 800-107; Recommendation for Applications Using Approved Hash Algorithms, August 2012
- [**ENISA**] Algorithms, key size and parameters, November 2014
- [**PKCS 1**] RSA Cryptography Standard
- [**ANSI X9.31**] Digital Signatures Using Reversible Public Key Cryptography
- [**ANSI X9.62**] The Elliptic Curve Digital Signature Standard (ECDSA)
- [**ANSI X9.82**] Random Number Generation Standard

APPENDIX

Acronyms

- **ANSI**: American National Standards Institute
- **ANSSI**: French Network and Information Security Agency
- **BSI**: German Federal Office for Security
- **DSA**: Digital Signature Algorithm
- **ECDSA**: Elliptic Curve Digital Signature Algorithm
- **Ecrypt II**: European Network of Excellence for Cryptology II
- **ETSI**: European Telecommunications Standards Institute
- **FIPS**: Federal Information Processing Standard
- **MAC**: Message Authentication Code
- **NIST**: National Institute of Standards and Technology
- **RSA**: Rivest, Shamir, Adleman
- **SHA**: Secure Hash algorithm
- **SP**: Special Publication