GM

CRYPTOGROPHIC INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0018-2023

Replacing GM/T 0018-2012

Cryptographic device application interface specification

密码设备应用接口规范

Issued on: December 04, 2023 **Implemented on: June 01, 2024**

Issued by: State Cryptographic Administration

Table of Contents

Foreword

This document was drafted in accordance with the provisions of GB/T 1.1-2020 "Directives for standardization - Part 1: Rules for the structure and drafting of standardizing documents".

This document replaces GM/T 0018-2012 "Cryptographic device application interface specification". Compared with GM/T 0018-2012, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

a) CHANGE the ECC key pair protection structure (see 5.9; 5.8 of the 2012 edition);

b) DELETE the two interface functions of digital envelope conversion based on RSA algorithm and digital envelope conversion based on ECC algorithm (see 6.3.7, 6.3.17 of the 2012 edition);

c) ADD 17 interface functions related to multi-packet symmetric encryption and decryption, multi-packet MAC calculation, single-packet authentic encryption and decryption, multi-packet authentic encryption and decryption (see 6.5; 6.5 of the 2012 edition);

d) ADD 3 interface functions related to hashing with keys (see 6.6);

e) ADD the verification and debugging functions (see 6.8);

f) DELETE Chapter 7 "Security requirements" (see Chapter 7 of the 2012 edition);

g) ADD the error codes when user identification does not match (see Appendix A);

h) ADD the definitions of 15 interface functions related to the SM9 identification cryptographic algorithm and the SM9 identification cryptographic algorithm (see Appendix B);

i) ADD the definitions of 6 interface functions for calculating IKE working keys, calculating IPSEC session keys, calculating SSL working keys (see Appendix C).

Please note that some contents of this document may involve patents. The issuing agency of this document does not assume the responsibility for identifying patents.

This document was proposed by AND shall be under the jurisdiction of the Cryptography Industry Standardization Technical Committee.

Drafting organizations of this document: China Electronics Technology Network Security Technology Co., Ltd., Wuxi Jiangnan Information Security Engineering Technology Center, Sichuan University, Beijing Guomai Information Security Technology Co., Ltd., Geer Software Co., Ltd., Beijing Digital Certification Co., Ltd., Xingtang Communication Technology Co., Ltd., Shandong De'an Information

Cryptographic device application interface specification

1 Scope

This document specifies the algorithm identification, data structure, interface function of the server-side cryptographic device application interface, under the public key cryptographic infrastructure application technology system.

This document is applicable to the development and use of server-side cryptographic devices, as well as application development based on such cryptographic devices.

2 Normative references

The contents of the following documents constitute the essential terms of this document through normative references in the text. Among them, for referenced documents with dates, only the versions corresponding to the dates are applicable to this document; for referenced documents without dates, the latest versions (including all amendments) are applicable to this document.

GB/T 15852.2 Cybersecurity technology - Message authentication codes (MACs) - Part 2: Mechanisms using a dedicated hash-function

GB/T 35276 Information security technology - SM2 cryptographic algorithm usage specification

GB/T 36624 Information technology - Security techniques - Authenticated encryption

GB/T 38635 (all parts) Information security technology - Identity-based cryptographic algorithms SM9

GM/T 0006 Cryptographic application identifier criterion specification

GM/T 0022 IPSec VPN technical specification

GM/T 0024 SSL VPN Specification

GM/Z 4001 Cryptographic terminology

3 Terms and definitions

The terms and definitions as defined in GM/Z 4001, as well as the following terms and

definitions, apply to this document.

3.1

Private key access password

Password used to verify the right to use the private key.

3.2

User key

Asymmetric key stored inside the device for application cryptographic operations, including signature key pairs and encryption key pairs.

4 Abbreviations

The following abbreviations apply to this document.

ECC: Elliptic Curve Cryptography

EPK: External Public Key

IPK: Internal Public Key

ISK: Internal Private Key

KEK: Key Encrypt Key

5 Algorithm identifier and data structure

5.1 Definition of algorithm identifier

The algorithm identifiers of the algorithms used in this document are given in GM/T 0006. The algorithm identifier of the block cipher algorithm includes its working mode.

5.2 Definition of basic data type

The basic data types in this document are stored and exchanged in Big-Endian format. Table 1 defines the basic data types.

obtain the plaintext of the private key of the ECC key pair.

6 Device interface description

6.1 Position of the cryptographic device application interface in the public key cryptographic infrastructure application technology system framework

In the public key cryptographic infrastructure application technology system framework, the cryptographic device service layer consists of cryptographic machines, cryptographic cards, intelligent cryptographic terminal devices. It provides basic cryptographic services to the general cryptographic service layer through the cryptographic device application interface specified in this document, as shown in Figure 1.

Basic cryptographic services include key generation, single cryptographic operations, file management services.

This document uses C language to describe interface functions. Unless otherwise specified, the length unit of the parameters in the function is the number of bytes. Cryptographic devices that comply with this document shall support the function interfaces of the ECC algorithm (ECC in this document specifically refers to the SM2 algorithm), symmetric algorithms, hash operations in this document. All interface functions listed in this document shall be able to be called arbitrarily by the application system. Appendix A defines the function return code; Appendix B defines the SM9 algorithm-related data structure and interface functions; Appendix C defines the VPN device-related interface functions.

When the product supports the SM9 algorithm, the SM9 algorithm-related data structure and interface functions shall comply with the definition in Appendix B. When the product supports VPN, the VPN device-related interface functions shall comply with the definition in Appendix C.

This is an excerpt of the PDF (Some pages are marked off intentionally)

------ The End ------