

Translated English of Chinese Standard: GM/T0016-2023

www.ChineseStandard.net → Buy True-PDF → Auto-delivery.

Sales@ChineseStandard.net

GM

CRYPTOGRAPHY INDUSTRY STANDARD
OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0016-2023

Replacing GM/T 0016-2012

**Smart token cryptography application interface
specification**

智能密码钥匙密码应用接口规范

Issued on: December 04, 2023

Implemented on: June 01, 2024

Issued by: State Cryptography Administration

Table of Contents

Foreword	3
Introduction	5
1 Scope	6
2 Normative references	6
3 Terms and definitions	6
4 Abbreviations	7
5 Structural model	7
5.1 Hierarchical relationship	7
5.2 Application structure of the device.....	8
6 Data type definitions	9
6.1 Algorithm identifiers	9
6.2 Basic data types.....	9
6.3 Constant definitions	10
6.4 Composite data types	10
7 Interface functions	18
7.1 Device management	18
7.2 Access control	21
7.3 Application management.....	24
7.4 File management	26
7.5 Container management.....	29
7.6 Cryptographic services.....	31
7.7 Verification and debugging	48
8 Interface usage requirements	51
8.1 Equipment usage phase	51
8.2 Permission management.....	52
8.3 Other security requirements	53
Annex A (normative) Definitions for error codes.....	54
Annex B (normative) SM9 application interface	56
Annex C (normative) VPN relative interfaces	71
Annex D (informative) SM9 programming examples	80
Bibliography	84

Foreword

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

This document replaces GM/T 0016-2012 "Smart token cryptography application interface specification". Compared with GM/T 0016-2012, in addition to structural adjustments and editorial changes, the main technical changes are as follows:

- a) Deleted "padding method" (see Table 11 of this Edition; Table 11 of Edition 2012);
- b) Changed the "modify device authentication key" function (see 7.2.2 of this Edition; 7.2.2 of Edition 2012);
- c) Changed "get container type" (see 7.5.7 of this Edition; 7.5.7 of Edition 2012);
- d) Changed "export public key" (see 7.6.18 of this Edition; 7.6.17 of Edition 2012);
- e) Changed "import session key" (see 7.6.19 of this Edition; 7.6.18 of Edition 2012);
- f) Changed "security requirements" (see Chapter 8 of this Edition; Chapter 8 of Edition 2012);
- g) Added HMAC-related interfaces (see 7.6.36, 7.6.37, 7.6.38, and 7.6.39 of this Edition);
- h) Added verification and debugging interfaces (see 7.7 of this Edition);
- i) Added SM9 application interfaces (see Annex B of this Edition);
- j) Added VPN-related interfaces (see Annex C of this Edition);
- k) Added SM9 programming examples (see Annex D of this Edition)

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. The issuing authority shall not be held responsible for identifying any or all such patent rights.

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

The drafting organizations of this document: Beijing Hitech Fangyuan Technology Co., Ltd., Beijing Wuqi Intelligent Technology Co., Ltd., Geer Software Co., Ltd., Wuxi Jiangnan Information Security Engineering Technology Center, Beijing Digital Certification Co., Ltd., Xingtang Communication Technology Co., Ltd., Shandong De'an Information Technology Co., Ltd., Beijing Sanwei Information Security Technology Development Co., Ltd., Shandong University, Beijing Daming Wuzhou

Smart token cryptography application interface specification

1 Scope

This document specifies the smart token cryptography application interface standard under the public key cryptography system, the functions, data types, parameter definitions of the cryptographic-related application interface, and the security requirements of the equipment.

This document applies to the development, use and testing of smart token products.

2 Normative references

The following referenced documents are indispensable for the application of this document. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

GM/T 0006-2023, *Cryptographic application identifier criterion specification*

GM/T 0017-2023, *Smart token cryptography application interface data format specification*

GM/T 0027-2014, *Technique requirements for smart token*

GM/T 0028-2014, *Technique requirements for smart token*

GM/Z 4001, *Cryptographic terminology*

PKCS#1, *RSA Cryptography specification version 2.1*

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GM/Z 4001 as well as the followings apply.

3.1 container

A unique storage space in a cryptographic device used to store keys.

3.2 terminal device

A general term for smart tokens.

3.3 device authentication

Smart token authentication for applications.

3.4 device authentication key

Key used for device authentication.

3.5 device label

The alias of the terminal device that can be set by the user and stored in the device.

3.6 administrator PIN

Administrator's password, as an ASCII string.

3.7 user PIN

User's personal password, as an ASCII string.

3.8 application

A structure consisting of containers and files with independent management permissions.

4 Abbreviations

The following abbreviations apply to this document.

API: Application Programming Interface

ASCII: American Standard Code for Information Interchange

MAC: Message Authentication Code

PKI: Public Key Infrastructure

PIN: Personal Identification Number

5 Structural model

5.1 Hierarchical relationship

The smart token application interface is located between the smart token application

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

Full-copy PDF can be purchased from 1 of 2 websites:

1. <https://www.ChineseStandard.us>

- SEARCH the standard ID, such as GB 4943.1-2022.
- Select your country (currency), for example: USA (USD); Germany (Euro).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Tax invoice can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with download links).

2. <https://www.ChineseStandard.net>

- SEARCH the standard ID, such as GB 4943.1-2022.
- Add to cart. Only accept USD (other currencies - <https://www.ChineseStandard.us>).
- Full-copy of PDF (text-editable, true-PDF) can be downloaded in 9 seconds.
- Receiving emails in 9 seconds (with PDFs attached, invoice and download links).

Translated by: Field Test Asia Pte. Ltd. (Incorporated & taxed in Singapore. Tax ID: 201302277C)

About Us (Goodwill, Policies, Fair Trading...): <https://www.chinesestandard.net/AboutUs.aspx>

Contact: Wayne Zheng, Sales@ChineseStandard.net

Linkin: <https://www.linkedin.com/in/waynezhengwenrui/>

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