GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040

L 80

File No.: 44628-2014

GM/T 0027-2014

Technique requirements for smart token

智能密码钥匙技术规范

Issued on: February 13, 2014 **Implemented on: February 13, 2014**

Issued by: State Cryptography Administration

Table of Contents

Foreword 3

1 Scope 4

2 Normative references 4

3 Terms and definitions 5

4 Abbreviation 7

5 Functional requirements 8

6 Hardware requirements 10

7 Software requirements 10

8 Performance requirements 11

9 Security requirements 11

10 Environmental adaptability requirements 13

11 Reliability requirements 14

Annex A (normative) Algorithm performance requirements 15

Bibliography 17

Technique requirements for smart token

1 Scope

This Standard specifies functional requirements, hardware requirements, software requirements, performance requirements, security requirements, environmental suitability requirements and reliability requirements for smart token.

This Standard is applicable to guide the research, development, testing and use of smart token. It is also used to guide the testing of smart token.

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.

GB/T 4208-2008, *Degrees of protection provided by enclosure (IP code)*

GB/T 17964, *Information technology - Security techniques - Modes of operation for a block cipher*

GM/T 0002, *SM4 Block Cipher Algorithm*

GM/T 0003, *Public Key Cryptographic Algorithm SM2 Based on Elliptic Curve*

GM/T 0004, *SM3 Cryptographic Hashing Algorithm*

GM/T 0005, *Randomness Test Specification*

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

GM/T 0009, *SM2 Cryptography Algorithm Application Specification*

GM/T 0016, *Smart token cryptography application interface specification*

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

5 Functional requirements

5.1 Initialization

The initialization of smart token includes:

- exit-factory initialization: initialization is required for device authentication key in exit-factory;
- application initiation: when the application provider distributes the device, it needs to modify the device authentication key and establish the corresponding application (the parameters to be set include the administrator password, user password, the number of containers in the application, the maximum number of key pairs in the application, the maximum number of certificates that the application needs to support, the maximum number of containers that can be created by the application).

5.2 Functional requirements for cryptographic operation

5.2.1 Block cipher algorithm

The smart token must support SM4 block cipher algorithm. Its realization shall meet the requirements of GM/T 0002.

The work mode of block cipher algorithm shall at least include two modes: electronic code book (ECB) and cipher block chaining (CBC), in accordance with the requirements of GB/T 17964.

The identifier of block cipher algorithm shall meet the requirements of GM/T 0006.

5.2.2 Public key cryptographic algorithm

The smart token must support SM2 public key cryptographic algorithm. Its realization shall meet the requirements of GM/T 0003.

The identifier of public key cryptographic algorithm shall meet the requirements of GM/T 0006.

The use of SM2 public key cryptographic algorithm by smart token shall meet the requirements of GM/T 0009.

5.2.3 Cryptographic hash algorithm

The smart token must support SM3 cryptographic hash algorithm. Its realization shall meet the requirements of GM/T 0004.

The identifier of cryptographic hash algorithm shall meet the requirements of

numbers are similar or not, whether the random number has better 0, 1 balance.

5.4 Device management

The smart token shall have device management functions, for example, device authentication key update, application deletion, application creation. The device management functions shall meet the requirements of GM/T 0017.

5.5 Device self-test

The device self-test functions mainly include firmware integrity, correctness of cryptographic algorithm, random number generator, algorithm coprocessor, storage key and data integrity check. It can be self-test when the device is powered on, and can also perform the corresponding self-check function by providing the corresponding function service for the upper-layer application.

Should the test fail, it shall return an error status code or physical alarm indication and stop working.

5.6 Other functions

Other functions such as application management, container management, file management, access control, key service shall meet the requirements of GM/T 0017.

6 Hardware requirements

6.1 Interface

The hardware interface of smart token shall at least support but not limited to one of the following interfaces: USB, SD, Dock, Lightning, Blue-tooth, NFC, audio, WiFi, ISO 7816, ISO 14443 or other interfaces.

6.2 Chip

The core chip of smart token needs the approval of the national cryptography management authority.

6.3 Line transfer

The line transfer protocol of smart token in the USB interface shall meet the requirements of GM/T 0017.

7 Software requirements

APDU command supported by smart token shall meet the requirements of GM/T 0017. If there is an extension instruction, it must be clearly stated in the

- password length should not be less than 6 characters; the number of times of logging in by using the wrong password shall not exceed 10 times;
- securely store and access password; the password stored inside the smart token cannot be output in any form;
- all passwords and keys transmitted between the management terminal and the smart token shall be encrypted; ensure that in the transmission process it can prevent replay attack.

c) the private key shall be secured during its generation, storage and use:

- the signature private key shall be generated inside the smart token, and cannot be output in any form;
- the encrypted private key must be ciphertext-encrypted and cannot be exported;
- the uniqueness of the private key shall be guaranteed; must not solidify the key pair and the prime number used to generate the key pair;
- the private key shall be stored and accessed in a secure manner; the private key cannot be leaked in any way during use;
- the smart token shall be subject to client identification before each sensitive operation such as signing; the identity authentication permission shall be cleared immediately after each sensitive operation such as signing.

d) the keys stored inside the smart token shall have effective key protection mechanisms that prevent anatomical, probing and illegal reads;

e) the smart token shall have the ability to resist various attacks, including but not limited to:

- energy analysis attacks, including simple energy analysis and differential energy analysis;
- electromagnetic analysis attacks, including simple electromagnetic analysis and differential electromagnetic analysis;
- time analysis attack;
- error injection attack.

f) in the event of changes in the external environment, the smart token shall not leak sensitive information or affect security features. Changes in the

Bibliography

[1] GB/T 2423.1-2008, *Environmental testing - Part 2: Test methods - Tests A: Cold*

[2] GB/T 2423.2-2008, *Environmental testing - Part 2: Test methods - Tests B: Dry heat*

[3] GB/T 2423.8-2008, *Environmental testing for electric and electronic products Part 2:Test methods Test Ed: Free fall*

[4] GB/T 2423.3-2008, *Environmental testing for electric and electronic products - Part 2: Testing method test Cab: Damp heat Steady state*

[5] GB/T 2423.10-2008, *Environmental testing for electric and electronic products - Part 2: Tests methods - Test Fc: Vibration (sinusoidal)*

[6] GB/T 17626.2-2006, *Electromagnetic compatibility (EMC) - Testing and measurement techniques - Electrostatic discharge immunity test*

[7] JR/T 0068-2012, *General Specification for Information Security of On-line Banking System*

_____ END _____

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

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