GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.030

CCS L 80

GM/T 0123-2022

Cryptography test specification for time stamp server

时间戳服务器密码检测规范

Issued on: November 20, 2022 **Implemented on: June 01, 2023**

Issued by: State Cryptography Administration

Table of Contents

Cryptography test specification for time stamp server

1 Scope

This document specifies the test contents, test requirements and test methods for time stamp servers.

This document applies to the cryptography test of time stamp server devices and the development of such cryptography devices. It can also be used to guide the development of applications based on such cryptography devices.

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 9813 (all parts) General specification for computer

GB/T 20518 Information security technology - Public key infrastructure - Digital certificate format

GB/T 20520-2006 Information security technology - Public key infrastructure - Time stamp specification

GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm

GB/T 32918 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves

GB/T 33560 Information security technology - Cryptographic application identifier criterion specification

GB/T 35275 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification

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

GM/T 0005 Randomness test specification

GM/T 0033-2014 Interface specifications of time stamp

GM/T 0039 Security test requirements for cryptographic modules

GM/T 0050 Cryptography device management - Specification of device management technology

GM/T 0062 Random number test requirements for cryptographic modules

GM/Z 4001-2013 Cryptology terminology

3 Terms and definitions

For the purpose of this document, the terms and definitions defined in GM/Z 4001 and the following apply.

3.1

time stamp

Data obtained by signing time and other data to be signed, used to indicate the time attribute of the data.

3.2

application entity

The service object of the time stamp server. It can be an individual, an organization or a system.

3.3

time stamp server

A server that provides accurate and reliable time stamp services based on PKI (Public Key Infrastructure) technology.

3.4

smart card

An integrated circuit card containing a CPU (central processing unit) and implementing cryptographic operations and key management.

4 Abbreviations

For the purpose of this document, the following abbreviations apply:

API: Application Programming Interface

HTTP: Hyper Text Transfer Protocol

5) cryptographic components or modules that have been certified by commercial cryptographic test, such as encryption cards, security chips, etc.

b) The time stamp server shall support the following main components or interfaces:

1) human-computer interaction components;

2) redundant power supply;

3) manual key destruction switch;

4) serial port;

5) timing antenna.

6.2 Function test

6.2.1 Initialization function test

The time stamp server shall have the initialization function to realize the conversion from the initial status to the ready status of the device.

The initialization operation of the time stamp server mainly includes the initial configuration of the system, the initialization of the administrator or operator, and the initial key generation (or recovery) and installation. Only after the initialization operation is completed can the cryptography service be provided. The time stamp server that has been initialized can automatically enter the ready status and provide cryptography services.

6.2.2 Device self-test test

The time stamp server shall have the self-test function. The self-test shall include power-on/reset self-test, periodic self-test and self-test after receiving instructions, test of the software and hardware status of the cryptography components, algorithms, random numbers, etc. of the time stamp server itself, including algorithm correctness test, random number generator test, stored key and data integrity test, and key component correctness test. After the self-test is completed, the self-test results shall be reported. If the self-test is successful, the time stamp server shall enter the management status or working status. If the self-test fails, the time stamp server shall report the self-test results and stop providing cryptography services to the outside.

6.2.3 Cryptographic operation test

6.2.3.1 Asymmetric algorithm test

The time stamp server shall support at least SM2 asymmetric algorithm to sign/verify data, and the curve parameters shall comply with the provisions of GB/T 32918.5. Cryptographic operations shall be completed in cryptographic components or modules

that have been certified by commercial cryptographic test, and shall support given keys and messages to be signed, and test the correctness of their operation results:

a) Use the given key to call the signature algorithm to sign the message to be signed, the test platform verifies the signature result, and the verification passes;

b) Use the given key to the correct signature result, call the signature verification algorithm to perform the signature verification operation, and the verification passes;

c) Use the given key to the wrong signature result, call the signature verification algorithm to perform the signature verification operation, and the verification fails.

6.2.3.2 Hash algorithm test

The time stamp server shall support at least SM3 algorithm to perform hash operations on messages, which shall comply with the provisions of GB/T 32905. The hash algorithm is called for a given message to calculate the hash value, and the result is exactly the same as the given hash value.

6.2.4 Key management test

The time stamp server shall have the complete key management function, which includes key generation, storage, use, update, backup, recovery, archiving and destruction. The security of the key in each link of the life cycle shall be guaranteed. The generation of the time stamp signature key pair shall use the cryptographic components or modules that has been certified by commercial cryptographic test, and the time stamp signature private key shall be securely stored in the cryptographic component or module.

6.2.5 Random number test

The time stamp server shall have the random number generation function. It shall use two or more independent chips with physical noise source function that have been tested and certified to realize the random number generation function. Collect 1000 random number files of 128 KB, test the collected random number files, and the test results shall meet the requirements of GM/T 0005.

The random number self-test shall comply with the power-on test and usage test requirements for Class E products in GM/T 0062; if the self-test fails, the cryptographic service shall be stopped, the device shall enter an error status and output an error indication.

6.2.6 Certificate management test

The test scope of the certificate management and verification function of the time stamp server includes the import, storage, verification, use, deletion, backup and recovery of

a) When calling the initialization environment interface, the time stamp server shall successfully establish the time stamp environment and return 0, otherwise it shall feedback the corresponding status code in Annex A of GM/T 0033-2014;

b) When calling the elimination environment interface, the time stamp server shall successfully clear the time stamp environment and return 0, otherwise it shall feedback the corresponding status code in Annex A of GM/T 0033-2014;

c) Use the correct cryptographic hash algorithm identifier to call the generate time stamp request interface, the time stamp server shall use the specified algorithm to perform cryptographic hash operations on the time stamp request information, successfully generate the time stamp request packet, and return 0; use the wrong cryptographic hash algorithm to call the generate time stamp request interface, it shall feedback the corresponding status code in Annex A of GM/T 0033-2014, and no time stamp request data is generated; the format of the time stamp request generated shall pass the test of 6.2.7.2;

d) Use the correct signature algorithm identifier to call the generate time stamp response interface, the time stamp server shall successfully generate a time stamp response packet according to the request packet, and return 0; use the wrong signature algorithm to call the generate time stamp response interface, it shall feedback the corresponding status code in Annex A of GM/T 0033-2014, and generate time stamp abnormal response data; the format of the time stamp response generated shall pass the test of 6.2.7.2;

e) Use the correct signature algorithm identifier and cryptographic hash algorithm identifier to call the time stamp validity verification interface, the time stamp server shall successfully verify whether the time stamp response is valid and return 0; use the wrong signature algorithm and cryptographic hash algorithm identifier to call the time stamp validity verification interface, it shall feedback the corresponding status code in Annex A of GM/T 0033-2014;

f) Use the time stamp main information acquisition interface, the time stamp server shall successfully acquire the main information of the time stamp and return 0, otherwise it shall feedback the corresponding status code in Annex A of GM/T 0033-2014;

g) Use the correct specified item number for obtaining time stamp details to call the parsing time stamp details interface, the time stamp server shall successfully parse the time stamp details and return 0; use the wrong item number to call the parsing time stamp details interface, it shall feedback the corresponding status code in Annex A of GM/T 0033-2014.

6.2.8 Trusted time source

The source of trusted time shall come from the national authoritative time department (such as the National Time Service Center), or the time obtained by the hardware and methods approved by the national authoritative time department.

One or more of the following methods can be used to obtain time.

a) Use a wireless receiving device to obtain the time issued by the national authoritative time department through wireless means, such as long-wave signals, satellite signals, etc.

b) Use a time synchronization protocol to obtain time from a specified network address. The time issued by the network address and the time synchronization protocol used shall be trustworthy and approved by the national authoritative time department.

c) Use a hardware certified by the national authoritative time department to obtain time, such as using an atomic clock.

The time stamp server shall be able to automatically synchronize time and be tested by using the management tool of the time stamp server. Time source synchronization shall meet the requirements of 6.3 in GB/T 20520-2006.

6.3 Management security test

6.3.1 Configuration management test

The time stamp server shall have the following main management functions:

a) Network address configuration function, which includes but is not limited to configuring IP address, subnet mask and gateway address;

b) Status management, which includes but is not limited to component status, software status, version status, current status;

c) Configuration management, which includes but is not limited to configuration management functions such as permission configuration and access control configuration.

The time stamp server permission configuration shall have:

a) no less than two types of role management, i.e., administrator and auditor;

b) administrators who are responsible for certificate management, access control, trusted time source configuration, etc. of the device;

c) auditors who are responsible for log management operations of the device.

6.3.2 Administrator management test

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

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