GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 44643-2014

GM/T 0038-2014

Key management of certificate authority system test specification

证书认证密钥管理系统检测规范

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

Issued by: State Cryptography Administration

Table of Contents

Foreword

This Standard was drafted in accordance with the rules given in GB/T 1.1-2009.

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

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

Main drafting organizations of this Standard: Changchun Jida Zhengyuan Information Technology Co., Ltd., Shanghai Gale Software Co., Ltd., National Information Security Engineering Technology Research Center, Beijing Haitai Fangyuan Science and Technology Co., Ltd.

Main drafters of this Standard: Liu Ping, Gao Li, Tian Jingqi, Jiang Yulin, Zhang Baoxin, Li Weiping, Zhao Lili, Zhu Guoxin, Yuan Feng, Tan Wuzheng, an Xiaojiang, Zhang Wantao, Wu Chenghua.

Key management of certificate authority system test specification

1 Scope

This Standard specifies the test contents and methods of the key management of certificate authorization system.

This Standard is applicable to providing electronic authentication service for electronic signature. The certificate authentication key management system developed or built according to GM/T 0034-2014 can also provide reference for the test of other certificate authorization key management systems.

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 0034-2014 Specifications of cryptograph and related security technology for certification system based on SM2 cryptographic algorithm

3 Terms and definitions

The following terms and definitions apply to this document.

3.1 Certificate authentication system; CA

The system of full life cycle management of digital certificates, such as the issuance, publication, updating and revocation of digital certificates.

3.2 Key management system; KM

A system to realize key management.

3.3 SM2 algorithm

An Elliptic Curve Public key cryptographic algorithm with a key length of 256 bits.

The main security strategies of intrusion detection configured to system are:

a) Deploy intrusion detection device on the switch of key service area to ensure detection of all external packets;

b) The intrusion detection management console shall be directly connected with the intrusion detection device to ensure its independent management and detection;

c) Set intrusion detection to high alert level of packets detection and analysis;

d) There shall be corresponding response strategies of security events detected by the intrusion detection devices;

e) The feature repository for intrusion detection shall be updated in a timely manner.

Note: Intrusion detection devices can also be set up as intrusion prevention devices.

7.2.2.3 Vulnerability scanning

The main security strategies of vulnerability scanning configured for the system are:

a) Conduct vulnerability scanning for critical server equipment, network equipment and network security devices regularly;

b) There shall be corresponding response strategies for security events detected by vulnerability scanning;

c) The vulnerability repository shall be updated in a timely manner.

7.2.2.4 Virus control

The main security strategies for the virus control configured for the system are:

a) Deploy antivirus products to key servers and operations, management terminals;

b) There shall be corresponding response strategies for security events detected by antivirus products;

c) The virus repository shall be updated in a timely manner.

7.2.2.5 Cryptographic machine

The cryptographic machine shall be connected to the server via an independent physical port.

The cryptographic machine shall be the product approved by the national cryptographic management department.

7.8 Data backup and recovery

There shall be data backup and recovery strategy to realize the data backup and recovery of key management system.

This article applies to item test only.

7.9 Third-party security products

7.9.1 Firewall

The deployment location of the firewall shall conform to the requirements of 7.1.2.

The firewall configuration strategies shall meet the requirements of 7.2.2.1.

The firewall products shall be products that qualify the inspection and certification of the relevant national institutions.

This article applies to item testing only.

7.9.2 Intrusion detection

The deployment location of the intrusion detection product shall comply with the requirements of the 7.1.2.

The configuration strategy of intrusion detection product shall meet the requirements of 7.2.2.2.

Intrusion detection products shall qualify the inspection and certification of the relevant national institutions.

This article applies to item test only.

Note: This article also applies to intrusion prevention products.

7.9.3 Vulnerability scanning

The deployment location of the vulnerability scanning product shall comply with the requirements of 7.1.2.

The configuration strategy of vulnerability scanning product shall meet the requirements of 7.2.2.3.

The vulnerability scanning product shall qualify the inspection and certification of the relevant national institutions.

This article applies to item test only.

7.9.4 Virus control

Count the keys in the standby, working and history repository, and the results shall meet the requirements of 7.6.2.5.

8.6.3 Log

Sort or search the log according to time, personnel, operation type respectively. The results shall meet the requirements of 7.6.3.

8.6.4 Audit

Perform audit operation in the audit interface on the information of the time of the event, the operator of the event, the type of operation, the result of the operation, the recorded signature and others. The results shall meet the requirements of 7.6.4.

8.6.5 Authority management

Perform in the access management interface operations of add or delete business administrators, setting business administrator access. The results shall meet the requirements of 7.6.5.

8.7 System performance

Test according to 7.7 and record test results.

8.8 Data backup and recovery

Review backup and recovery strategies and corresponding measures, which shall comply with requirements of 7.8.

8.9 Third-party security products

Check firewall, intrusion detection (intrusion prevention), vulnerability scanning and virus control product deployment and corresponding product certification, which shall meet the requirements of 7.9.

8.10 Documents

View documents accompanied to certificate authentication key management system. They shall meet the requirements of 7.10.

9 Qualification determination

9.1 Item qualification determination

7.1.2, 7.2.1, 7.2.2.5, 7.6.2.1, 7.6.2.3 are key items. If any one of the test results does not meet the requirements of the corresponding test, it shall be determined as unqualified.

Appendix A

(Informative)

Test outline

A.1 Test objective

Test if products or items comply with GM/T 0034-2014.

A.2 Physical areas and network structure of key management system

Attach drawings to show the layout of the computer room, equipment location, physical connection and network structure.

A.3 Hardware and software configuration of key management system

Describes the type and configuration of software and hardware products used in the test environment.

A.4 Module and function of key management system

Describe the main modules and functions of the key management system. (Drawings can be attached).

A.5 Test content

A.5.1 Site

For site test, see table A.1.

Table A.1 -- Site test

No.	Test Content	Test Method	Expected result	Test result	Conclusion
1	Access Control	Use authorized device (such as: access card) to enter	Enter granted		
2		Use unauthorized device (such as: access card) to enter	Enter rejected		
3	Monitor	Check real time monitoring	Conform to standard		
4		Check multiple screen monitoring	Conform to standard		
5		Check history record of monitoring	Conform to standard		

			increase accordingly		
9		Generate spare key in real time: pre-generate a specified number of keys, check the number of keys in the standby repository	Pre-generate correctly and the number of keys increase accordingly		
10	Key recovery	In the key recovery interface, recover by authorized forensic personnel and operator with key recovery authorization to recovery the key	Successfully recovery the key		
11	Key revocation	After CA provided key revocation service, check the status of working repository	Status of working repository changes accordingly		
12	Key statistics	Working key statistics: execute working key statistics	Display result, acquire the current working key number		
13		Spare key statistics: execute spare key statistics	Display result, acquire the current spare key number		
14	Log	Sort or comprehensively search the log by time, personnel and operation type, acquire result	Display the corresponding page		
15	Audit	Search by any combination condition set: if the log list conforming to the condition exists, display the log list; if do not exist, return null.	Display the corresponding page		
16		Verify the recorded signature	Can verify		
17		Mark the audited records	Can mark		

A.5.6 System performance

For system performance test, see table A.6.

Table A.6 -- System performance test

No.	Test Content	Test Method	Expected result	Test result	Conclusion
1	System performance	Generate a specified number of keys, count the keys generated per second	Acquire key generation time		

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

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