GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 44642-2014

GM/T 0037-2014

Certificate authority system test specification

证书认证系统检测规范

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.

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.

Certificate authority system test specification

1 Scope

This Standard specifies the test contents and methods of certificate authority system.

This standard is applicable to provide electronic authentication service for electronic signature and the inspection of development or building of certificate authentication service operation system in accordance with GM/T 0034-2014. It can also provide reference for the inspection of other certification 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/T0014 Digital certificate authentication system cryptography protocol specification

GM/T 0015 Digital certificate format based on SM2 algorithm

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

A system that manages the entire life cycle of digital certificates such as issuing, distributing, updating, and revoking them.

3.2 Registration authority; RA

The main function of registration authority that manages the entire process of digital certificate registration. It is also known as registration system.

3.3 CA certificate

A certificate issued to a CA. It can be issued by the CA to itself or by another CA.

The item test environment is the actual environment of the certificate authority system.

8 Test content

8.1 Site

8.1.1 Engineering construction

Engineering construction shall meet the requirements of physical security in 8.5 of GM/T 0034-2014.

8.1.2 Physical areas

The physical area of certificate authority system shall be divided into public area, service area, management area and core area.

The storage and distribution server of certificate/ certificate logoff list, the LDAP / OCSP query server (if there is an OCSP query server) and the connected cryptographic machine, the registration management server and the connected cryptographic machine, intrusion detection or intrusion prevention detection equipment, vulnerability scanning equipment shall be located in server area; registration management terminal, registration audit terminal, certificate/ certificate logoff list generation and issuance management terminal, intrusion detection or intrusion prevention management console shall be located in the management area; the generation and issuance server of certificate/ certificate logoff list and the connected cryptographic machine, database server, the safe-box keeping key backup materials and media shall be placed in the core area; Firewall shall be placed between each of the areas. See Appendix C.

The core area shall be the shielded computer room. The shielding effect shall meet the requirements of 8.5.2.5 in GM/T0034-2014.

The sequence of entering each area is: the management area, service area, core area.

The device's name in the system shall be labeled at a prominent location on the devices placed in each area, such as issuance server, registration server, etc.

Monitoring probe, fire probe and access control system shall be set up in each area; and monitor room shall be set up to monitor each area in real time.

This article applies to item test only.

8.2 Network

8.2.1 Network structure

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.

8.2.2.4 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.

8.2.2.5 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.

8.3 Post and access management

8.3.1 Issuance system

8.3.1.1 Super administrator

The super administrator shall be set up, which is generated when the system is initialized and is responsible for the strategy management of the system and the management of the business administrators of the system.

8.3.1.2 Audit administrator

The audit administrator shall be set up, which is generated when the system is initialized and is responsible for the auditor management of the system.

8.3.1.3 Business administrator

The business administrator shall be set up and authorized by the super administrator. It is responsible for the management of business operators.

8.3.1.4 Business operator

The business operator shall be set up and authorized by the business administrator It is responsible for user certificate repository management, data backup/ recovery, etc.

8.6.1.1 Input of application information

It shall be able to provide the interface to input and modify the certificate application information. It shall be able to select the key type and length of the application digital certificate AND support the import of a batch of certificate application information. The system shall enable the operators to sign their actions automatically.

8.6.1.2 Review of application information

It shall be able to provide an interface for the review of the application information. It shall be able to read the application information that needs to be audited. It shall be able to submit the approved information to the issuing system and return the unapproved information to the input interface. The system shall enable the operators to sign their actions automatically.

8.6.1.3 Certificate download

It shall be able to provide an interface for downloading certificates, and to download safely the certificate information. The system shall be able to enable operators to sign their actions automatically.

8.6.1.4 Authority management

It shall be able to provide an interface for business administrators to manage business. The business administrator shall be able to add, delete operators and assign their accesses through the interface.

8.6.1.5 Certificate template update management

When the certificate template for CA to authorize RA changes, RA shall be able to update the template synchronously with CA.

8.6.1.6 Log

The log shall record the time of the event, the operator of the event, the type of operation and the result of the operation.

It shall be able to sort or be inquired according to time, operator and operation type.

8.6.1.7 Audit

A separate audit management terminal shall be set up to provide an interface for audit management. It shall be able to audit information about the time of the event, the operator of the event, the type of operation and the result of operation. Audit shall be able to verify the signature of the record.

Audit data shall be archived and not tampered with.

The deployment location of virus control product shall comply with the requirements of 8.1.2.

The configuration strategy of virus control product shall comply with the requirement of 8.2.2.4.

The virus control product shall be inspected and certified by relevant state agencies.

This article applies to item test only.

8.10 Entry into root

The certification system product shall support connection to national root CA.

The operating certification system shall be connected to the national root CA.

8.11 Certificate format

The certificate format shall conform to the requirements of GM/T 0015 and GM/T 0034-2014.

8.12 Certificate chain

Ensure the validity of the certificate chain.

8.13 Algorithm

Certification systems shall be able to issue digital certificates using the SM2 algorithm and other algorithms approved by the national cryptographic management authority.

Digital certificates shall be based on SM2 algorithm or other algorithms approved by the national cryptographic management authority.

8.14 Protocol

The protocol adopted by the certification system shall conform to the requirements of GM/T 0014.

8.15 Documents

The certification system shall be accompanied with relevant documentation in accordance with the requirements of GM/T 0034-2014.

9 Test method

9.1 Site

9.1.1 Engineering construction

9.3 Management of posts and authorization

9.3.1 Insurance system

9.3.1.1 Super administrator

If log on to the super administrator interface in the right way, the system shall approve.

If log on to the super administrator interface in the wrong way, the system shall disapprove.

9.3.1.2 Audit administrator

If log on to the audit administrator interface in the right way, the system shall approve.

If log on to the audit administrator interface in the wrong way, the system shall disapprove.

9.3.1.3 Business administrator

If log on to the business administrator interface in the right way, the system shall approve.

If log on to the business administrator interface in the wrong way, the system shall disapprove.

9.3.1.4 Business operator

If log on to the business operator interface in the right way, the system shall approve.

If log on to the business operator interface in the wrong way, the system shall disapprove.

9.3.1.5 Auditor

If log on to the auditor interface in the right way, the system shall approve.

If log on to the auditor interface in the wrong way, the system shall disapprove.

9.3.2 Registration authority

9.3.2.1 Business administrator

If log on to the business administrator interface in the right way, the system shall approve.

If log on to the business administrator interface in the wrong way, the system shall disapprove.

9.10 Entry into root

Check the CA certificate issuer and verify its validity.

9.11 Certificate format

Check the each of the contents of the certificate, which shall comply with the requirements of 8.11, and verify its validity.

9.12 Certificate chain

Verify the validity of the certificate chain and comply with the requirements of 8.12.

9.13 Algorithm

Check the algorithms in the cryptographic device used by the CA, which shall include the SM2 algorithm.

Check certificate authentication system optional algorithms, which shall meet the requirements of 8.13.

The specified algorithm shall be able to issue digital certificate successfully.

9.14 Protocol

The protocol used by the certification system, which shall comply with the requirements of 8.14.

9.15 Documents

Check the documents accompanied to the certification system, which shall comply with the requirements of 8.15.

10 Qualification determination

10.1 Item qualification determination

8.1.2, 8.2.1, 8.2.2.5, 8.6.2.3, 8.6.2.2, 8.10, 8.11, 8.12, 8.13, 8.14 are the key items. Any one of the test results that does not meet the corresponding test requirements shall be determined as unqualified.

8.6.2.3 and 8.6.2.7 are combined key items. If both test results fail the requirements of the corresponding test, it shall be determined as unqualified.

Except for above items, if the failing results of other items accumulate up to 5 (including 5 items), 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 certificate authority 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 certificate authority system

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

A.4 Module and function of certificate authority system

Describe the main modules and functions of the certificate authority 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		

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

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