GM

CRYPTOGRAPHY INDUSTRY STANDARD

OF THE PEOPLE'S REPUBLIC OF CHINA

ICS 35.040
L 80
File No.: 44635-2014

GM/T 0034-2014

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

基于 SM2 密码算法的证书认证系统密码及相关安全技术规范

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

Issued by: State Cryptography Administration

Table of Contents

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

1 Scope

This standard specifies the specifications of cryptograph and related security technology for digital certificate authentication system based on SM2 cryptographic algorithm, including certificate authentication center, key management center, cryptography algorithm, cryptography device and interfaces.

This standard applies to guide the construction and detection assessment of the digital certificate authentication system of the third-party authority, standardize the application of cryptograph and related security technology in digital certificate authentication system. The construction, operation and management of the digital certificate authentication system of the non-third-party authority may refer to this standard.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 2887 General specification for computer field

GB/T 6650 Technical conditions for movable floor of computer room

GB/T 9361 Safety requirements for computer field

GB 50174 Code for design of electronic information system room

GM/T 0014 Digital certificate authentication system cryptography protocol specification

GM/T 0015 Digital certificate format based on SM2 algorithm

GM/T 0016 Smart token cryptography application interface specification

- Online certificate status inquiry: The user or application system queries the status of a certificate online in real time in accordance with the OCSP protocol defined in RFC 6960.

In practical applications, it can use either or both of above two inquiry methods depending on the circumstances.

5.2.6 Certificate management system

The certificate management system is a management control system which realizes the functions of application, audit, generation, issuance, storage, distribution, revocation and archiving of certificate/certificate revocation list in certificate authentication system.

5.2.7 Security management system

Security management system includes security audit system and security system.

Security audit system provides event-level audit function, for tracking, counting and analyzing of records related to system security, personnel, time.

Security system provides access control, intrusion detection (intrusion prevention), vulnerability scanning, virus prevention and other network security features.

5.3 System design

5.3.1 Overview

The design of certificate authentication system includes the overall design of the system and the design of each subsystem. This standard provides the design principles of certificate authentication system and the realization methods of each subsystem. In the specific realization process, it shall perform detailed design based on the selected development platform and development environment.

5.3.2 Overall design principles

The overall design principle of certificate authentication system is as follows:

a) Certificate certification system follows the standardized and modular design principles;

b) The certificate authentication system sets up relatively independent function modules, realizing various functions through the secure connection between each module;

5.3.4 Certificate/certificate revocation list generation and issuance system design

5.3.4.1 Certificate/certificate revocation list generation and issuance system functions

The certificate/certificate revocation list generation and issuance system are the core of the certificate authentication system. It not only provides the service of certificate issuance/certificate revocation lists for the entire certificate authentication system, but also undertakes the main security management in the entire certificate authentication system.

Its main functions are as follows:

- Certificate generation and issuance: The user information is read and verified from the database, and the encryption key pair is applied to the key management center in accordance with the type of the certificate to be issued, to generate the user's signature certificate and the encryption certificate, and the certificate that has been issued is released to the directory server and database. Depending on the system's configuration and management policies, different signature keys can be used for different types or usages of certificates.

- Certificate update: The system shall provide CA certificate and user certificate update function.

- Certificate revocation list generation and issuance: Receive the revocation information, verify the signature in the revocation information, and then issue a certificate revocation list, and issue the issued revocation list to the database or the directory server. The signature key issuing the certificate revocation list may be the same or different from the signature key that issues the certificate.

- Security audit: Be responsible for the inquiry, counting, and statement printing of the operation log of the administrator and operator of the certificate/certificate revocation list generation and issuance system.

- Security management: Perform secure access control for the login to the certificate/certificate revocation list generation and issuance system, and manage and back up the certificate/certificate revocation list database. Set up administrators and operators and apply and download digital certificates for these personnel. Configure different cryptography devices; configure different certificate templates.

The certificate/certificate revocation list generation and issuance system shall have the ability to process in parallel.

- CRL inquiry. The user or application system uses the CRL address identified in the certificate to inquire and download the CRL to the local and verify the status of the certificate.

- Online certificate status inquiry. The OCSP protocol is used by the user or application system to check the status of the certificate online in real time. The inquiry result is signed and returned to the requester for verification of the certificate status.

5.3.6.2 Certificate status inquiry system structure

The certificate status inquiry system is composed of certificate status database/OCSP server, security management module, security audit module and cryptography device.

a) Certificate status database/OCSP server

Accept the certificate status inquiry request of the users and application systems, in accordance with the certificate serial number in the request information, inquire the certificate status from the certificate status database, the inquired result is returned to the requester.

b) Cryptography device

Verify the signature in the request message and sign the inquiry result.

c) Security management

It mainly includes:

1) The configuration of the OCSP server; defining the acceptable access control information and the address of the inquired certificate status database;

2) Start/stop the inquiry service. Configure the number of acceptable user requests, and so on.

d) Security audit

Inquire the security audit log in the certificate status inquiry system, perform statistics and printing.

5.3.7 Certificate management system design

The certificate management system is a comprehensive information control and scheduling service system of the certificate authentication system. It receives various kinds of request information from users and submits the request information to the corresponding subsystems. The certificate management

evidence data.

b) Security system

Provide access control, intrusion detection (intrusion prevention), vulnerability scanning, virus prevention and other network security features.

5.4 Digital certificate

For the structure and format of digital certificates, see GM/T 0014 and GM/T 0015.

Among them, the DN sequence of the issuer name and principal name in the certificate structure shall comply with the following rules:

- If there is a C item, then put it in the end, and C = CN;
- If there is a CN item, put it at the front of the DN;
- If both OU item and O item exist at the same time, OU is placed in front of O; if both S item and L item exist at the same time, L is placed in front of S.

The cryptography algorithm identified in the signature algorithm field in the certificate structure must be an algorithm approved by the national cryptographic management authority.

5.5 Certificate revocation list

The certificate revocation list structure and format in this standard is as shown in GM/T 0014 and GM/T 0015.

The certificate revocation list distribution point in the certificate shall be a valid address.

Among them, the cryptography algorithm identified in the signature algorithm field in the certificate revocation list structure must be an algorithm approved by the national cryptography administration department.

6 Key management system

6.1 Structure description

Key management system consists of key generation, key management, key

expired or is revoked to the historical key library.

- Process the key in the history key library, transfer the key exceeding the specified retention period to the prescribed carrier.

- Receive and examine the applications for key recovery, process it in accordance with the security policy;

- Authenticate the identity and authority of the relevant operations and operators in this system.

6.3.5 Key library management module

6.3.5.1 Overview

The key library management module is responsible for the key storage management. In accordance with the state of the key library it stores, the key library is divided into the standby library, the in-service library, and history library, the key data in the key library must be encrypted and stored.

6.3.5.2 Standby library

Standby library stores the key pair to be used. Key generation module pre-generates a number of key pairs, which are stored in the standby library; when required by CA, they can be promptly called to CA and then transferred into the in-service library.

The standby key library shall maintain a certain number of standby key pairs. The number of stored keys depends on the number of users in the system. If less than the set minimum quantity, it shall automatically make up to the specified quantity.

6.3.5.3 In-service library

The in-service library stores the in-service key pairs. In the in-service library, the key record contains the user's certificate serial number, ID number and valid time and other signs.

6.3.5.4 History library

History key library stores the expired or revoked key pair. The key record in the history library contains the user's certificate serial number, ID number, valid time, expiration date, and other signs.

6.3.6 Authentication management module

The authentication management module is responsible for the authentication of the identity and authority of the operations and operators that enter the system.

The following administration and operation staff shall be set up in the CA:

- Super administrator;
- Auditor administrator;
- Auditor;
- Business administrator
- Business operator.

The “super administrator” is responsible for the policy setting of the CA system, setting the business administrators of each subsystem and authorizing the business scopes managed by them.

The “business administrator” is responsible for the business management of a subsystem of the CA system, setting up the business operator of the subsystem and authorizing the authority of its operation.

“Business operator” conducts specific business operations in accordance with their authority.

“Audit manager” is responsible for producing and managing the auditors.

“Auditor” is responsible for auditing and overseeing the incidents involving the security of the system and the behavior of various administration and operations staff.

The above types of personnel use the certificate to log in, including “super administrator” and “audit administrator” certificate which shall be generated at the time of initialization of CA system.

In addition, CA shall set up security administrator, to be fully responsible for the system security.

8.1.4 Network division

CA system computer network needs reasonable segmentation, in principle requires that the entire network shall be divided into four parts z

a) Public part: It is the network where CA users are located, all users will access the CA through this network;

b) Service part: Provide domain name resolution function for external users and responsible for internal system’s sending and receiving external mail. It includes various Web servers and slave directory servers of the system. It is the interface for external users to access internal functions and

measures.

8.2.3 Communication security

The main objective of communication security is to ensure the secure communication between subsystems of CA system, CA and KMC, CA and RA. Security measures such as communication encryption and secure communication protocol shall be adopted.

8.2.4 Key security

8.2.4.1 Overview

The key goal of key security is to secure the keys used in the CA system throughout its lifecycle, including generation, storage, use, update, abolition, archiving, destruction, backup, and recovery. It shall take a variety of security measures such as hardware cryptography device, key management security protocol, key access control, key management operation audit.

8.2.4.2 Basic requirements

The basic requirements of key security are:

a) The generation and use of the key must be finished in a hardware cryptography device;

b) The generation and use of the key must have a safe and reliable management mechanism;

c) All keys that exist outside the hardware cryptography device must be encrypted;

d) The key must have a safe and reliable backup and recovery mechanism;

e) The operation of the cryptography device must be performed by multiple operators.

8.2.4.3 Root CA key

The root CA key security, in addition to meeting basic requirements, shall also satisfy the following requirements:

a) Root CA key generation

The root key of the CA system is generated by the hardware cryptography device and stored in the cryptography device. The key share shall be shared by the (5, 5) secret sharing mechanism with the five persons in charge.

Core area shall be shielded room, it shall be installed with high-strength steel security door. All lines access to shielded room shall take anti-electromagnetic leakage measures. Shielding effect shall meet the requirements of class C in BMB 3-1999.

Note: Class-C requirements in BMB 3-1999 are consistent with Class C requirements in GJB 5792-2006 “Classification and measurement methods of electromagnetic shielding systems for military confidential information systems”.

8.5.2.6 Security monitoring and distribution fire fighting

CA shall set security monitoring room, system monitoring room, distribution room and fire device room.

Security monitoring room is a place for security management personnel on duty, which can monitor all the personnel access to the CA and handle the daily security event. The security management personnel can only enter with both the identification card and the human characteristic identification, and leave by swiping the card.

System monitoring room is where network administrators work. It can only be accessed with both the identification card and human identification, and left by swiping the card.

Distribution room is to place all the power supply device, only the corresponding authorized personnel can enter with both identification card and human characteristics, and leave by swiping the card.

Fire-fighting device room is a room where fire-fighting device is stored. It is recommended to use an ID card to enter the fire-fighting device room.

8.5.3 Access control and physical intrusion alarm system

CA shall set access control and physical intrusion alarm system.

Access control system controls the access to the doors of all levels. Staff need to use ID card or combined with the human identification to access, and access to each door shall have corresponding time records and related information prompt.

Any unlawful intrusion, unauthorized opening of doors, and unauthorized personnel retention after the authorized personnel had been swiped card and left the room shall trigger an alarm system. Alarm system shall clearly indicate the alarm location.

Access control and physical intrusion alarm systems shall be provided with UPS and shall provide power supply for at least 8 hours.

9.7 Personnel management system

KMC personnel management system makes reference to the requirements of clause 8.6.

10 Certificate authentication center operation and management requirements

10.1 Personnel management requirements

To prevent unauthorized personnel from operating the CA system, an operator authentication system shall be provided on each operator terminal, and the relevant operators shall be subject to identity authentication and authorization control for all operations of the system.

Each operator in the CA system is equipped with a certificate carrier (such as smart token) that identifies the personal identification information. The certificate carrier has a cryptography protection mechanism to ensure the security of the private key.

The operator includes the following types:

a) CA super administrator: Its authority is to add, delete, change the CA business administrator account.

b) CA service administrator: Its authority is to add, delete, change CA business operator account.

c) CA service operator: Its authority is to manage the certificate template, configure the certificate policy, and configure the system. For example, configure the host encryption server parameters, directory server, CA system parameters, and RA system parameters. Add, delete, change RA business administrator and RA auditor account.

d) CA audit administrator: Its authority to add, delete, change the CA auditor account.

e) CA auditor: Responsible for querying CA system logs and querying audit CA operation records.

f) RA service administrator: Its authority is to add, delete and change RA service operator account.

related documents shall be formulated and be carried out after the approval of the supervisor. There shall be a double presence in the operation;

c) When the system fails, it shall be checked and handled by the system administrator. Other personnel shall not be handled without approval;

d) Unauthorized installation of any software and hardware on the server is not allowed;

e) It shall not delete any files on the server without approval.

10.2.3.2 Data backup

Data backup operation and maintenance specifications shall include the following:

a) After the system is upgraded, full backup shall be performed immediately;

b) For servers with large data changes, make incremental backups once a day and full backup once a week;

c) For servers with small data changes, backup can be made once a week;

d) Two sets of backups of important data shall be prepared, of which one is to be kept in another place;

e) The backup of the database shall be done separately;

f) The backup of important directory shall be done separately;

g) For manual backup, the media shall be marked of the backup server and path;

h) For automatic backup, backup media shall be effectively distinguished;

i) The selected backup medium shall ensure the long-term reliability of the data, otherwise it shall be regularly updated.

10.2.3.3 Password management

Password management specifications shall include the following:

a) The password length shall be more than 8 bytes. It shall be a combination of letters, numbers and special characters. Numbers and phrases with special meaning (such as name, birthday, telephone number, etc.) shall not be used as password;

b) Password strength security shall be checked when setting password;

a) CA system design: Describe the logical structure, network structure, data communication design, key management, business process flow and system hardware and software configuration of CA system.

b) CA system security: Describe the CA system to ensure the security of CA by adopting such measures as firewall, intrusion detection (intrusion prevention), vulnerability scanning, virus prevention and control, access control and security configuration. At the same time, describe the realization of the CA security measures from the data communications, key management, certificate management, security audit, physical security and other aspects.

c) CA system installation and configuration manual: Describes the installation and configuration of the CA system.

d) CA system security objectives: Describe whether the CA system meets the national safety standards.

e) CA system user manual: A technical manual describing the user's use and operation of the CA system.

10.6.3 Physical construction class

Physical construction class includes two types of files: physical field security manuals, physical field security management provisions, physical construction class files mainly describe the follows:

a) Physical field security manual: Describe the requirements and realization of physical security at physical fields;

b) Physical field security management provisions: Describe personnel's authority to enter and exit various areas of CA, the reception and management of visitors, the use of access control systems and the operation of monitoring alarm systems.

10.6.4 Personnel management class

The personnel management class files mainly include two classes of files: trusted personnel policy, principle and identification of trusted personnel positions, the main contents of the personnel management files are described as follows:

a) Trusted personnel policy: Describe the trusted personnel policies and how to conduct trusted personnel investigations;

b) The principle and identification of trusted personnel positions: Describe the principle of trusted personnel positions, trusted personnel

requirements

11.1 Personnel management requirements

To prevent unauthorized personnel from operating the key management system, an operator identity authentication system shall be provided at each operation terminal, and the relevant operators shall be subject to identity authentication and authorization control for all operations of the system.

Each operator of the key management system is configured with a certificate carrier (such as smart token) that indicates information related to personal identity. The certificate carrier has a password protection mechanism to ensure the security of the private key.

The operator includes the following types:

a) KM super administrator: Its authority is to add, delete, change KM business operator account.

b) KM service operator: Its authority is generating key, storing key, backup key and recovering key.

c) KM audit administrator: its authority is to add, delete, change KM auditor account.

d) KM auditor: be responsible for creating, querying audit records or logs.

For all personnel, it must digitally sign their actions.

11.2 Operation management requirements

Perform in accordance with the requirements of 10.2.

11.3 Key management requirements

Perform in accordance with the requirements of 10.3.

11.4 Security management requirements

Perform in accordance with the requirements of 10.4.

b) Forensic investigators. Forensic investigators must hold a digital certificate that attests to their identity and key hardware that can perform digital signature (such as smart token).

Judicial key recovery process is as follows:

a) The key management center performs identity authentication for the forensic personnel, after passing authentication, it can enter the next step.

b) If the encryption certificate corresponding to the encryption key pair to be recovered has not expired or has not been revoked, the key management center service operator finds the encryption key pair to be recovered in the in-service library; if the encryption certificate corresponding to the encryption key pair to be recovered has expired or has been revoked, the operator finds the encryption key pair to be recovered in the history library.

c) Digital envelopes can be made using the public key of forensic officers, and the encryption key pair to be recovered can be stored in a digital envelope. The SM2 encryption key pair protection structure can also be used to store the recovered encryption key pair. The SM2 encryption key pair protection structure data format can be found in GM/T 0016.

d) Save the recovered encryption key as a digital envelope or as an encryption key protection structure file in a forensic carrier, such as smart token.

e) Forensic officers and key center operators involved in the recovery must digitally sign the judicial key recovery record.

12.6 Certificate suspension process

The certificate holder, the law or the government authority may request that the certificate be suspended, a certificate suspension request shall be made to the RA, the RA service operator shall review the suspension request, and if rejected, inform the reason for the failure, and if accepted, the RA service operator will send the digital certificate to be suspended and the suspension request to the CA system, CA system adds this certificate information to the CRL list, and change the status of this certificate on the OCSP response server into “revoked”.

12.7 Release certificate suspension process

The certificate suspension proposer submits a request for releasing the certificate suspension to the RA, the RA service operator audits the suspension release request, if rejected, inform the reasons of failure; if accepted, the RA

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

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