

ICS 35.040

GM

**INDUSTRY STANDARD OF THE
PEOPLE'S REPUBLIC OF CHINA**

GM/T 0074-2019

**Technical requirements on cryptographic application for
internet banking**

网上银行密码应用技术要求

(English Translation)

Issued on: July 12, 2019

Implemented on: July 12, 2019

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Abbreviations	3
Overview	4
Data integrity requirements	5
Non-repudiation requirements	6
Verification audit requirements	7
Key revocation and archiving	8
Overview	9
Certificate lifecycle management	10
Interface requirements	11
General requirements	12
Security requirements for server-side cryptographic devices	13
Overall requirements	14

1 Scope

This standard specifies relevant requirements for the application of cryptographic technology in internet banking, including six aspects:

cryptographic algorithms, key management, certificate management, secure channels, cryptographic device, digital signatures.

This standard is applicable to guide the design, implementation and use of cryptographic technology-related security functions in internet banking. The testing and management of cryptographic sub-systems in internet banking systems may refer to it.

Relevant parts of mobile banking systems can also 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 15843 (All parts) Information technology - Security techniques -Entity authentication

GB/T 19713 Information technology - Security techniques - Public key infrastructure - Online certificate status protocol GB/T 20518 Information security technology - Public key infrastructure - Digital certificate format GB/T 28447 Information security technology - Specification on the operation management of a certificate authority GB/T 32905 Information security technology SM3 cryptographic hash algorithm GB/T 32907 Information security technology - SM4 block cipher algorithm GB/T 32915 Information security technology - Binary sequence randomness detection method GB/T 32918 (all parts) Information security techniques - Elliptic Curve public - key cryptography GB/T 35275 Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification GB/T 35276 Information security technology - SM2 cryptography algorithm usage specification GM/T 0015 Digital certificate format based on SM2 algorithm GM/T 0016 Smart token cryptography application interface specification GM/T 0017 Smart token cryptography application interface data format specification GM/T 0018 Interface specifications of cryptography device application GM/T 0019 Universal cryptography service interface specification GM/T 0021 One time password application of cryptography algorithm GM/T 0022 IPsec VPN specification GM/T 0023 IPsec VPN gateway product specification GM/T 0024 SSL VPN specification GM/T 0025 SSL VPN gateway product specification GM/T 0027 Technique requirements for smart token GM/T 0028 Security requirements for cryptographic modules GM/T 0029 Sign and verify server technical specification GM/T 0030 Cryptographic server technical specification GM/T 0033 Interface specifications of time stamp GM/T 0034 Specifications of cryptograph and related security technology for certification system based on SM2 cryptographic algorithm GM/T 0037 Certificate authority system test specification GM/T 0038 Key management of certificate authority system test specification 3.5 Server the provider of financial business services in the internet banking system.

4 Abbreviations

The following abbreviations apply to this document.

CSP: Cryptographic Service Provider IPSEC: Internet Protocol Security OTP: One Time Password PKCS: Public Key Cryptography Standards SSL: Secure Socket Layer TLS: Transfer Layer Secure VPN: Virtual Private Network WTLS: Wireless Transport Layer Security

5 Overview

The cryptographic application technology system of Internet banking is a security service system based on cryptographic technology. It uses cryptographic technology to support features such as authenticity, confidentiality, integrity, non-repudiation, to form a secure support for internet banking systems and services, so as to protect its application security and secure operation. Cryptographic devices based on cryptographic algorithms, key

management, digital certificates, secure channels, digital signatures and other cryptographic technologies provide security guarantees for internet banking systems, thus support the secure deployment of internet banking business. The support of cryptographic application technology for internet banking is as shown in Figure 1.

them, when using the cryptographic algorithm of GB/T 32918, it shall follow the requirements of GB/T 35275 or GB/T 35276.

7.1.3 Data integrity requirements

The data exchanged between the customer and the internet banking system shall be checked for integrity, to prevent third party modification. The data that needs to be checked for integrity include, but are not limited to: the login data, transaction application data, and contract data sent by the customer from the local bank to the internet banking system; as well as the login results, query results, transaction results, contract results as sent from the online banking system to the client.

In order to ensure the integrity of the data, it shall be digitally signed, hashed, or other similarly processed. According to the application scenario, use the cryptographic algorithm of GB/T 32918, GB/T 32905, GB/T 32907, or as approved by the national cryptographic authority. Among them, when using the cryptographic algorithm of GB/T 32918, it shall follow the requirements of GB/T 35275 or GB/T 35276.

7.1.4 Non-repudiation requirements

The transactions and contracting activities performed by customers after logging in to the internet banking system require that both the bank and the customer cannot be denied: the customer cannot deny the finished transfer records or contract records, etc.; the bank cannot deny the finished transfer, contract, and other operations.

In order to ensure the non-repudiation of the actions of both parties, it shall make digital signature of the action information. According to the application scenario, use a cryptographic algorithm approved by GB/T 32918 or the national cryptographic authority.

7.1.5 Verification audit requirements

Verification audit mainly includes two aspects: in-process verification audit and post-process verification audit. In-process verification audit is to verify or audit whether the client's identity and authority are legal during the operation of the internet banking system by the customer. It mainly includes system login, identity authentication and authority checking in transactions. post-process verification audit is to verify or audit the correctness of the transaction data stored in the background of the internet banking system.

To ensure the operability and security of the verification audit, before audit, it should encrypt or shield the key fields such as name, account number, amount in the audit target.

If encryption is adopted, it shall use the cryptographic algorithm of GB/T 32918, GB/T 32905, GB/T 32907, or as approved by the the working key inside the device can be backed up in the security area of the device. When the device detects that the working key has been illegally changed, the device shall recover the key. It is forbidden to provide external access interfaces in the secure area of key work and storage, to prevent key leakage.

When an external backup of the key is required, it shall be protected by security hardware, or exported in cipher text after the key is encrypted; it shall not be exported directly in plain text.

7.2.6 Key revocation and archiving

Expired, obsolete or leaked keys shall be updated in a timely manner. The original keys can be archived but shall no longer be used.

7.3.1 Overview

Digital certificates used in internet banking mainly refer to digital certificates used by end users to complete identity authentication, secure communication, and transaction signatures.

The construction of certificate authentication systems and related key management systems shall follow the requirements of GM/T 0028, GM/T 0034, GM/T 0037, GM/T 0038, GM/T 0039, GM/T 0054, GB/T 28447 and other related standards.

The certificate format shall follow the requirements of GB/T 20518 and GM/T 0015.

The online certificate status service shall comply with the requirements of GB/T 19713.

7.3.2 Certificate lifecycle management

The certificate lifecycle includes the following phases:

- a) Certificate application: When an internet banking customer applies for a certificate, the bank reviews the application information and identity information submitted by the user, to confirm that it is complete, authentic, valid.
- b) Certificate downloading: During the certificate downloading process, the private key generated by the asymmetric key pair inside the smart key shall be protected by the smart key at all times; the externally-derived key pair shall be encrypted and protected, to prevent private key disclosure;
- e) Cryptographic hashing operation: Single-packet or multi-packet hash generation;
- f) Message authentication code calculation: Single-packet or multi-packet message authentication code generation and verification;