

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

GM/T 0072-2019

**Technical requirements for the applying of cryptography in
remote mobile payment**

远程移动支付密码应用技术要求

(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
Certificate authority; CA	3
Client software	4
One time password; OTP	5
SMS dynamic code	6
Digital certificate	7
Digital signature	8
Overview	9
Data confidentiality	10
Data integrity	11
Identity authentication	12
Non-repudiation	13
Key storage	14
Key use	15
Key update	16
Key destruction	17
Device data confidentiality guarantee requirements	18
Device non-repudiation guarantee requirements	19
Device cryptographic algorithm requirements	20
Cryptographic equipment security requirements	21
Key use	22
Key update	23
Key archiving	24
Platform-side identity authentication guarantee requirements	25
Platform-side non-repudiation guarantee requirements	26
Platform-side cryptographic algorithm requirements	27

1 Scope

This Standard describes the architecture for the applying of cryptography in remote mobile payment based on the cryptographic module and specifies the cryptographic security

elements of remote mobile payment and the technical requirements for the applying of cryptography.

This Standard is applicable to providing guidance on cryptographic security elements to be considered and technical requirements to be followed for the applying of cryptography in cryptographic module-based remote mobile payment.

2 Normative references

The following documents are indispensable for the application of this document.

For the dated references, only the editions with the dates indicated are applicable to this document. For the undated references, the latest edition (including all the amendments) are applicable to this document.

GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32907 Information security technology - SM4 block cipher algorithm GB/T 32915 Information security technology - Randomness test methods for binary sequence GB/T 32918 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves 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 GB/T 37092 Information security technology - Security requirements for cryptographic modules the system used to manage all aspects of the life cycle of key such as generation, loading, storage, backup, distribution, update, archiving, and destruction.

3.8 Certificate authority; CA

The issuing authority of certificate, i.e. the authority responsible for issuing certificates, certifying certificates, and managing issued certificates. It is responsible for formulating policies and specific steps to verify and identify users and signing user certificates, to ensure the identity of certificate holders and the ownership of public key. It is also known as the certification center.

3.9 Client software

The application that implements financial payment functions on mobile device.

3.10 One time password; OTP

It means that it is used only once in the authentication process; another password is used for the next authentication; each password is used only once.

One time password authentication currently has three technical modes: based on time synchronization mechanism, based on event synchronization mechanism, and based on

challenge/response (asynchronous) mechanism.

3.11 SMS dynamic code

Also known as SMS password, which is a random number sent by the background system to the user's bound mobile phone in the form of a mobile phone text message. The user is authenticated by replying to the random number.

3.12 Digital certificate

Also known as public key certificate, a data structure signed by a certificate authority (CA) and containing public key owner information, public key, issuer information, validity period, and extended information. According to category, it can be divided into personal certificate, authority certificate, and equipment certificate. According to purpose, it can be divided into signature certificate and encryption certificate.

3.13 Digital signature

The result obtained by the cryptographic operation of the signer using the private key to the hash value of the data to be signed. The result can only be verified with the public key of the signer, which is used to confirm the integrity authority (CA). If other authentication modes are used (such as OTP, etc.), the cryptography platform includes a key management system and other cryptography platforms. The key management system provides key management services for the cryptographic module on the platform side. A certificate authority is an authority that provides certificate authentication services. In the process of applying of cryptography in remote mobile payment, if a certificate authentication mode is not used, only a key management system is required; if a certificate authentication mode is used, a certificate authority is also required to provide certificate authentication services.

6.1 Overview

The security requirements for applying of cryptography are mainly the data confidentiality, integrity, identity authentication, and non-repudiation in remote mobile payment processes.

6.2 Data confidentiality

Transaction sensitive data, during the process of client application input, storage on the mobile device side, transmission between the mobile device side and the platform side, storage on the platform side, and transmission between different system platforms on the platform side, cannot be obtained in plain text by unauthorized entities and thus used or leaked.

6.3 Data integrity

The data transmitted between the client application and the cryptographic module, the data transmitted between the mobile device and the remote payment system, and the data transmitted between the remote payment system and other system platforms cannot be modified or destroyed without authorization.

6.4 Identity authentication

In remote mobile payment, the identity of each entity shall be confirmed, to prevent identity from being occupied or impersonated.

6.5 Non-repudiation

In remote mobile payment, it shall be ensured that the sending entity of transaction information cannot falsely deny the message it sent afterwards.

7.3.2.2 Key storage

If the symmetric key or SM2 private key needs to be stored, it must be securely stored in the cryptographic module of the mobile device, to ensure the security of key storage and prevent key leakage and illegal replacement.

When the cryptographic module of mobile device is invalidated, the stored key must be invalidated with it.

7.3.2.3 Key use

Keys need to specify attributes, to prevent unauthorized use or misuse of keys.

Key use requirements:

- a) The key can only be used for the specified application;
- b) The key can only be used for the specified purpose or function;
- c) When a known key is compromised, it shall be discontinued;
- d) When it is suspected that a key is compromised, it is possible to actively stop using it.

7.3.2.4 Key update

It shall be possible to update the key according to the key update policy.

7.3.2.5 Key destruction

According to the key management policy, the key can be destroyed. The key to be destroyed is required to be destroyed from various used media. The destruction result is