

ICS 35.040
CCS L 80

GM

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

GM/T 0094-2020

**Public key cryptographic application technology framework
specification**

公钥密码应用技术体系框架规范

(English Translation)

Issued on: December 28, 2020

Implemented on: July 1, 2021

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Attribute authority system	4
Access control	5
Certificate authentication system	6
Cryptography device service	7
Common cryptography application support	8
Series of specifications within the framework	9

1 Scope

This Document specifies the public key cryptographic application technology framework. It gives the components and their logical relationships within the framework.

This Document is applicable to the construction of public key cryptographic application technology system and the formulation as well as revision of related standards. It guides the cryptographic application of the application system.

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.

GB/T 35275, Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification GM/Z 4001, Cryptographic terms

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GM/Z 4001 as well as the followings apply.

3.1 Attribute authority system

a management system that is used to generate, issue, update and revoke attribute certificates

3.2 Access control

according to a specific policy, a mechanism to allow or deny users access to resources

3.3 Certificate authentication system

framework

4.2 Cryptography device service

The cryptography device service is composed of cryptographic modules. The cryptographic module includes cryptographic machines, cryptographic cards, smart cryptographic terminals and other equipment or cryptographic software.

It provides key management, cryptographic calculation and device management services to the common cryptography application support through the cryptography device service interface. It accepts the cryptography device management of the infrastructure security support platform.

In the cloud computing environment, the cryptography device service consists of a cryptography device and a cryptography resource pool. The physical cryptography device is virtualized into virtual cryptography devices that shall be assigned to tenants on demand. In order to effectively manage virtual cryptographic resources, a cryptographic resource manager is required in the infrastructure security support platform to manage the creation, destruction, configuration and drift of cryptographic resources in the cryptography device service.

4.3 Common cryptography application support

The common cryptography service function mainly includes: being responsible to complete the security connection to the cryptography device; realize the identity authentication based on digital certificate, obtain relevant information from the certificate so as to implement security mechanisms such as authorization management and access control; being responsible for interacting with cryptography devices to implement specific cryptographic operations;

encapsulating the data according to the GB/T 35275 format, data encapsulation format has nothing to do with the application system, realizing application system interconnection and information sharing.

The common cryptography application support supports the interface through the common cryptography application. It provides the upper layer (typical cryptography application support and application) with transparent cryptographic application support that has nothing to do with specific cryptography devices. It transforms the upper-level cryptographic application support request into a specific basic cryptographic operation request. It calls the

corresponding cryptography device through a unified cryptography device application interface to implement specific cryptographic calculations and key operations.

The common cryptography application support includes cryptographic functions such as certificate analysis, certificate authentication, confidentiality, integrity, authenticity and non-repudiation of information.

4.7 Series of specifications within the framework

The series of standards within this framework include but are not limited to:

a) Cryptography device (1):

GM/T 0017, Smart token cryptography application interface data format specification GM/T 0022, IPsec VPN specification GM/T 0024, SSL VPN 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

b) Cryptography device service to common cryptography application support (2):

GM/T 0016, Smart token cryptography application interface specification GM/T 0018, Interface specifications of cryptography device application the interface naming and error code interval division involved in the interface specification shall be carried out in accordance with Annex A and Annex B.

c) Common cryptography service (3):

GM/T 0009, SM2 Cryptography Algorithm Application Specification GM/T 0010, SM2 cryptography message syntax specification

d) Common cryptography application support to the upper layer (4):

GM/T 0019, Universal cryptography service interface specification GM/T 0020, Certificate application integrated service interface specification

e) Authentication (5):

GM/T 0026, Security authentication gateway product specification

f) Electronic signature (6):

Annex C

(informative)

List of crypto industry standards in the framework that have been transformed into national standards the List of crypto industry standards in the framework that have been transformed into national standards is as follow:

- a) GM/T 0022 "IPSec VPN specification" corresponds to the national standard GB/T 36968-2018 "Information security technology - Technical specification for IPSec VPN";
- b) GM/T 0028 "Security Requirements for Cryptographic Modules" corresponds to the national standard GB/T 37092-2018 "Information security technology - Security requirements for cryptographic modules";
- c) GM/T 0016 "Smart token cryptography application interface specification" corresponds to the national standard GB/T 35291-2017 "Information security technology - Cryptography token application interface specification";
- d) GM/T 0009 "SM2 Cryptography Algorithm Application Specification" corresponds to the national standard GB/T 35276-2017 "Information security technology - SM2 cryptography algorithm usage specification";
- e) GM/T 0010 "SM2 cryptography message syntax specification" corresponds to the national standard GB/T 35275-2017 "Information security technology - SM2 cryptographic algorithm encrypted signature message syntax specification";
- f) GM/T 0015 "Digital certificate format based on SM2 algorithm" corresponds to the national standard GB/T 20518-2018 "Information security technology - Public key infrastructure - Digital certificate format";
- g) GM/T 0034 "Specifications of cryptograph and related security technology for certification system based on SM2 cryptographic algorithm" corresponds to the national standard GB/T 25056-2018 "Information security technology - Specifications of cryptograph and related security technology for certificate authentication system".