

ICS 35.030
CCS L 80

GM

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

GM/T 0120-2022

**Implementation guidance for electronic signature service based
on cloud computing**

基于云计算的电子签名服务技术实施指南
(English Translation)

Issued on: November 20, 2022

Implemented on: June 1, 2023

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Electronic signature	4
Cloud computing	5
Cloud service provider	6
Cloud service customer	7
Signer	8
Relying party	9
Cloud-based signing service	10
Collaborate signature mechanism	11
Delegated signature mechanism	12
Atomic operation	13
Abbreviations	14
General	15
Reference architecture	16
Cloud signature infrastructure	17
Add user	18
User registration	19
User information management	20
User freezing and unfreezing	21
User logout	22
Key hierarchy	23
Master key (SMK)	24

1 Scope

This document provides reference routes and methods for implementing electronic signature services based on cloud computing.

This document is applicable to the construction of electronic signature service systems based on cloud computing and the development of related products. It can be used as a reference for the testing and management of electronic signature service systems based on

cloud computing.

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 15843.3, Information technology -- Security techniques -- Entity authentication - Part 3: Mechanisms using digital signature techniques GB/T 15843.4, Information technology -- Security techniques -- Entity authentication - Part 4: Mechanisms using a cryptographic check function GB/T 20518, Information security technology -- Public key infrastructure -- Digital certificate format GB/T 25064, Information security technology -- Public key infrastructure -- Electronic signature formats specification GB/T 25069, Information security techniques -- Terminology GB/T 25070, Information security technology -- Technical requirements of security design for classified protection of cybersecurity GB/T 31168, Information security technology -- Security capability requirements for cloud computing services GB/T 32905, Information security techniques -- SM3 cryptographic hash algorithm GB/T 32907, Information security technology -- SM4 block cipher algorithm GB/T 32918.2, Information security technology -- Public key cryptographic algorithm SM2 based on elliptic curves - Part 2: Digital signature algorithm 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 36326, Information technology -- Cloud computing - General operational requirements of cloud service GB/T 37092, Information security technology -- Security requirements for cryptographic modules GB/T 38636, Information security technology -- Transport layer cryptography protocol (TLCP) GB/T 39786, Information security technology -- Baseline for information system cryptography application GM/T 0109-2021, Technical requirements for electronic signature service based on cloud computing GM/Z 4001, Cryptography terminology

3 Terms and definitions

For the purposes of this document, the terms and definitions defined in GB/T 25069, GM/T 0109-2021, GM/Z 4001 as well as the followings apply.

3.1 Electronic signature

Data contained or attached in electronic form in a data message that is used to identify the signer and indicate that the signer approves the content.

3.2 Cloud computing

A mode that provides access to scalable and flexible physical or virtual resource pools over the network and enables on-demand self-service resource acquisition and management.

NOTE: Resource examples include servers, operating systems, networks, software, applications, and storage devices.

3.3 Cloud service provider

Cloud computing service provider.

NOTE: Cloud service providers manage, operate, and support the computing infrastructure and software for cloud computing, and deliver cloud computing resources through the Internet.

3.4 Cloud service customer

Participants who establish business relationships with cloud service providers using cloud computing services.

NOTE: In this document, cloud service customer is referred to as customer.

3.5 Signer

The entity that creates the electronic signature.

3.6 Relying party

An entity that accepts a dependency agreement with a cloud-based signing service and independently determines whether the electronic signature meets the security requirements of its application.

3.7 Cloud-based signing service

Organizations that provide cloud-based electronic signature services and related services to other entities.

3.8 Collaborate signature mechanism

A mechanism that the signer and the cloud service each store part of the key component and complete the electronic signature through mutual cooperation.

3.9 Delegated signature mechanism

A mechanism that the signer hosts the key in the cloud service and authorizes the cloud service to complete the electronic signature.

3.10 Atomic operation

An operation or series of operations that cannot be interrupted.

4 Abbreviations

The following abbreviations apply to this document.

API. Application Programming Interface CA. Certificate Authority CPU. Central Processing Unit HTTPS. Secure Hypertext Transfer Protocol IMEI. International Mobile Equipment Identity IMSI. International Mobile Subscriber Identity IPsec. IP Security JSON. JavaScript Object Notation KEK. Key Encryption Key OTP. One Time Password PIN. Personal Identification Number SDK. Software Development Kit SMK. System Main Key SSL. Secure Socket Layer TLCP. Transport Layer Cryptography Protocol USK. User Signing Key VPN. Virtual Private Network

5 General

The electronic signature service based on cloud computing can be planned and implemented according to the network security level protection requirements of the relevant business systems and the requirements of GM/T 0109, and in accordance with the requirements of GB/T 39786 for the corresponding levels of physical and environmental security, network and communication security, equipment and computing security, and application and data security.

a) Choose a suitable physical location. Follow GB/T 25070 to build an infrastructure that matches the business security level. The infrastructure includes capabilities for physical and environmental security protection, meets the physical and environmental requirements of GB/T 39786, and provides the required cryptographic support capabilities for electronic signature service activities. If the electronic signature service provider uses physical and environmental facilities provided by a third party, it can be required to comply with the requirements of GB/T 39786 that are consistent with the network security level required by the business.

b) Through network partitioning and network protection technology, deploy firewalls, intrusion detection network protection, network isolation and other technologies or products. Take security control and access measures that match the business security level for different partitions. At the same time, take corresponding boundary protection and other mechanisms to meet the requirements of GB/T 39786 for network and communication security. If the electronic signature service provider uses network facilities provided by a third party, it can be required to meet the requirements of GB/T 39786 that are consistent with the network security level required by the business.

c) The requirements of GB/T 39786 for equipment and computing security are met through