

ICS 35.030
CCS L 80

GM

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

GM/T 0117-2022

**Technical requirements for cryptographic applications of
identity service in network**

网络身份服务密码应用技术要求

(English Translation)

Issued on: November 20, 2022

Implemented on: November 20, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Confidentiality	3
Integrity	4
Authenticity	5
Non-repudiation	6
General Requirements	7
Level 1	8
Level 2	9
Level 4	10
Level 1	11
Level 3	12
Level 4	13

1 Scope

This document stipulates the technical requirements for cryptographic applications of identity service in network for natural persons, provides network identity service model, network identity service security level, cryptographic application demands framework and cryptographic application security objective, and provides specific technical requirements for cryptographic applications of identity verification service, identity authentication service and identity federation service.

This document is applicable to the planning, design, development, deployment and application of cryptographic applications of identity service in network for natural persons.

2 Normative References

The contents of the following documents constitute indispensable clauses of this document through the normative references in the text. In terms of references with a specified date, only versions with a specified date are applicable to this document. In terms of references without a specified date, the latest version (including all the modifications) is applicable to this document.

GB/T 15843 (all parts) Information Technology - Security Techniques - Entity Authentication
GB/T 22239 Information Security Technology - Baseline for Classified Protection of

Cybersecurity GB/T 25069 Information Security Techniques - Terminology GB/T 35273
Information Security Technology - Personal Information Security Specification GB/T 37036
(all parts) Information Technology - Biometrics Used with Mobile Devices GB/T 37092
Information Security Technology - Security Requirements for Cryptographic Modules GB/T
38556 Information Security Technology - Technical Specifications for One-time-password
Cryptographic Application GB/T 39786 Information Security Technology - Baseline for
Information System Cryptography Application GB/T 40660 Information Security Technology
- General Requirements of Biometric Information Protection

6.2 Confidentiality

Important data in network identity services (such as: identity authentication information, sensitive personal information and authenticator keys, etc.) will not be obtained by unauthorized entities during the collection, storage, use and transmission, etc., and thus be exploited or leaked. Confidentiality is achieved using encryption and decryption techniques, etc.

6.3 Integrity

Important data in network identity services (such as: identity authentication information, sensitive personal information and authenticator keys, etc.) will not be modified or destroyed without authorization during the collection, storage, use and transmission, etc. Integrity is achieved using cryptographic technology, such as: message authentication code mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, and digital signature mechanisms based on public key cryptographic algorithms, etc.

6.4 Authenticity

In identity services in network, confirm the authenticity of the identities of participating entities to prevent identities from being appropriated or counterfeited. Authenticity is achieved using cryptographic technology, such as: message authentication code mechanisms based on symmetric cryptographic algorithms or cryptographic hash algorithms, digital signature mechanisms based on public key cryptographic algorithms, and dynamic password mechanisms, etc.

6.5 Non-repudiation

Participating entities in identity services in network cannot deny their data originating behavior and data receiving behavior in the network identity services. Non-repudiation is achieved using cryptographic technology, for example, digital signature mechanisms based on public key cryptographic algorithms.

7 Technical Requirements for Cryptographic Applications of Identity Service in Network

7.1 General Requirements

In identity proofing service, identity authentication service and identity federation service, Level 1 to Level 4 shall comply with the following general requirements:

- a) The cryptographic algorithms, cryptographic technology, cryptographic products and cryptographic services used in network identity services shall comply with the provisions of laws and regulations, and the relevant requirements of cryptography-related national standards and industry standards;
- b) The collection, storage, use, entrusted processing, sharing, transfer and public disclosure of personal information, and the handling of personal information security incidents shall comply with the provisions of GB/T 35273, and the protection requirements for biometric features recognition shall comply with the provisions of GB/T 40660.

7.2.1 Level 1

The requirements for Level 1 are as follows.

- a) Requirements for identity proofing: real names are not required, and anonymous, pseudonymous or real names may be used.
- b) Requirements for communication protection: cryptographic technology may be adopted to ensure the integrity of data in the communication process; cryptographic technology may be adopted to ensure the confidentiality of important data in the communication process; cryptographic technology may be adopted to authenticate communication entities.
- c) Requirements for recording and storage:
 - 1) The identity service provider shall record and store the necessary information for the identity proofing service, including but not limited to collected user identity information and identification documents, process information generated by identity proofing, and proofing results, etc.;
 - 2) Cryptographic technology may be adopted to ensure the confidentiality and integrity of important data storage.
- d) Requirements for risk mitigation: see A.1 in Appendix A for possible risks.

Cryptographic technology may be adopted to mitigate possible risks.

- e) Requirements for system security protection: the network identity service system shall at least comply with Level 1 security requirements specified in GB/T 22239 and shall at least comply with Level 1 cryptographic application technical requirements specified in GB/T 39786.

7.2.2 Level 2

The requirements for Level 2 are as follows.

- a) Requirements for identity proofing: user identity shall be verified using any mode of remote identity proofing, in-person over remote channel identity proofing and in-person identity proofing, and real-name verification shall be performed.
- b) Requirements for communication protection: cryptographic technology may be used data storage, and cryptographic technology shall be adopted to ensure the confidentiality of important data storage.
- d) Requirements for risk mitigation: see A.1 for possible risks. When there are means of cryptographic technology that can mitigate risks, cryptographic technology shall be adopted to deal with the risks.
- e) Requirements for system security protection: the network identity service system shall at least comply with Level 2 security requirements specified in GB/T 22239 and shall at least comply with Level 2 cryptographic application technical requirements specified in GB/T 39786.

7.2.4 Level 4

The requirements for Level 4 are as follows.

- a) Requirements for identity proofing: user identity shall be verified using the mode of in-person identity proofing, and real-name verification shall be performed.
- b) Requirements for communication protection: cryptographic technology should be used to ensure the integrity of data in the communication process. Cryptographic technology should be adopted to ensure the confidentiality of important data in the communication process (such as: citizen identity numbers, addresses, and scanned copies of important documents, etc.), and cryptographic technology shall be adopted to perform two-way authentication on communication entities.
- c) Requirements for recording and storage:
 - 1) The identity service provider shall record and store the necessary information for the identity proofing service, including but not limited to the collected user identity information and identification documents, process information generated by identity proofing, and proofing results, etc.;
 - 2) Cryptographic technology shall be adopted to ensure the integrity and confidentiality of important data storage.
- d) Requirements for risk mitigation: see A.1 for possible risks. When there are means of cryptographic technology that can mitigate risks, cryptographic technology shall be adopted