ICS 35.240
CCS L 70

NATIONAL STANDARD OF THE PEOPLE'S REPUBLIC OF CHINA

GB/T 47702-2026

Blockchain and distributed ledger technology - General services - Technical requirements for decentralized identity systems

区块链和分布式记账技术 通用服务 分布式身份系统技术要求

Issued on: May 25, 2026 **Implemented on: September 1, 2026**

Issued by: State Administration for Market Regulation;
Standardization Administration of the PRC

Table of Contents

1 Scope

GB/T 47702-2026 is the Chinese national standard covering decentralized identity on a distributed ledger - the identifiers and the documents that resolve them, the verifiable credentials issued against them, the wallets that hold them, and the revocation and recovery that decide whether the scheme survives contact with real users. First edition, in force since 1 September 2026. It was issued on 25 May 2026 and has been in force since 1 September 2026, as a first edition. The document is under the responsibility of the Ministry of Industry and Information Technology. This page is published from the official record of the 2026 edition; the clause text of a standard this recent is not yet in circulation, and the figures, limits and tables it contains are those of the document itself, delivered in full with the English translation.

5.2 Service Interface Layer External application systems connect to the distributed identity system through a service interface layer, and the access methods include SDK, client, API, etc.

5 Distributed Identity System Architecture

5.1 Architecture The distributed identity system architecture (see Figure 1) includes a service interface layer, a distributed identity capability layer, an infrastructure layer, and a cross-functional layer.

a) The service interface layer includes the SDK, client, and API, which mainly realizes the interface and data exchange between the distributed core service and external systems. exchange;

b) The distributed identity capability layer includes a DID subsystem, a credential subsystem, and a verifiable data registration subsystem, primarily implementing distributed... The core functions of an identity system;

c) The infrastructure layer includes storage infrastructure and cryptographic infrastructure, providing the basic storage and cryptographic support for distributed identity systems. Serve;

d) The cross-functional layer includes a security management module, a governance module, and an auditing module, covering the service interface layer and distributed identity system. The identity capability layer and infrastructure layer are used to protect the security and privacy of user identity information in the distributed identity system, and to achieve the desired results. Identity-related behaviors are traceable and auditable, thereby enabling the entire ecosystem to operate transparently, compliantly, and efficiently. Figure

5.3 Distributed Identity Capability Layer

5.3.1 DID Subsystem The DID subsystem provides DID identifier and DID document management functions, including DID creation, parsing, use, update, recovery, and deregistration. Etc. The syntax structure related to DID identifiers is shown in Appendix A.

5.3.2 Voucher Subsystem The credential subsystem includes a VC module and a VP module, providing management functions for VCs and VPs, including VC issuance, verification, and updating. This includes cancellation, transfer, deletion, and the presentation and verification of VPs. Appendix B uses the process of logistics document and voucher transfer in a cross-border trade scenario as an example to illustrate this. This highlights the advantages of using a distributed identity system.

5.3.3 Verifiable Data Registration Subsystem The verifiable data registration subsystem includes a DID data registration module, a VC data registration module, and a VP data registration module, combined with the underlying... Storage infrastructure together constitutes VDR, providing secure data storage and access functions, and ensuring data immutability, traceability, and reliability. audit.

5.4 Infrastructure Layer The infrastructure layer of a distributed identity system includes storage infrastructure and cryptographic infrastructure.

a) Storage infrastructure provides data storage services for distributed identity systems, including distributed ledgers, trusted databases, etc., depending on the application. For different scenarios, decentralized distributed ledgers or centralized trusted databases can be chosen as the storage infrastructure;

b) Cryptographic infrastructure provides cryptographic services for distributed identity systems, including personal key devices or systems (TEE, SE, cryptographic modules). Blocks, etc.), key custody devices or systems (key vaults, key management systems, etc.), cryptographic computing devices (cryptographic machines, cryptographic cards). etc.

5.5 Cross-functional layer The cross-functional layer includes the security management module, governance module, and audit module.

a) The security management module is used to ensure the security and privacy protection of DID and VC identity information;

b) The governance module establishes a management framework and technical standards by designating a management body, thereby achieving transparency, compliance, and efficiency across the entire ecosystem. Operation;

c) The audit module records, monitors, and evaluates all operations in the system, ensuring that all identity-related behaviors are traceable, compliant, and secure.

6.Technical Requirements for Service Interface Layer Distributed identity systems provide services externally through SDKs, clients, APIs, etc., and meet the following requirements.

a) Measures should be taken to ensure the accuracy and reliability of data collected through the interface;

b) Measures should be taken to ensure the confidentiality of data transmission through the interface;

c) Measures should be taken to ensure the integrity of data transmission during interface data transfer;

7.1 DID Subsystem

7.1.1 DID Creation DID creation generates and associates DID identifiers and DID documents, meeting the following requirements.

a) It is advisable to generate DID public/private key pairs through a user agent;

b) A DID identifier should be created based on information such as the DID public key;

c) A corresponding DID document should be created based on the DID identifier, DID public key, etc.

d) The DID identifier and the DID document should have a one-to-one correspondence;

e) The uniqueness of the DID identifier should be ensured;

f) It is advisable to verify the authenticity of the DID subject's identity with an authoritative institution before creating the DID.

Note. The authoritative institution for verifying the authenticity of natural persons' identities

is the National Online Identity Authentication Public Service Platform.

7.1.2 DID Resolution DID parsing retrieves the DID document based on the DID identifier, and must meet the following requirements.

a) The DID document should be obtained by parsing the VDR based on the DID identifier;

b) Specific attributes in the DID document can be retrieved from the VDR;

c) The DID document corresponding to the specified version of the DID identifier can be parsed from the VDR.

7.1.3 DID Usage DID is used for signing or encryption using application DID, and must meet the following requirements.

a) Data should be digitally signed using the DID private key, and the signature should be verified using the corresponding DID public key;

7.2 Voucher Subsystem

7.2.1 VC Issuance The VC issuance process involves the issuer issuing VCs to the holder, and must meet the following requirements.

a) The holder should have created a DID identifier and corresponding DID document before the issuer issues the VC;

b) When a holder requests the issuance of a VC, they should digitally sign it using the private key corresponding to their DID identifier;

c) When issuing a VC, the issuer should use the public key corresponding to the holder's DID identifier to verify the digital signature in the VC issuance request. It is proven that he/she is the holder of the DID identifier;

d) After the identity attribute verification is successful, the issuer should use its private key to sign the holder's identity information and issue the VC;

e) It is advisable to load the VC template from the VDR and issue VC based on the VC template;

f) After issuing the VC, the issuer shall send the VC from the issuer to the holder via a secure channel;

g) It is advisable to use privacy-preserving technologies such as zero-knowledge proofs and Merkle trees to generate VCs.

7.2.2 VC Verification The VC validation process involves the validator verifying the validity of the VC, and it must meet the following requirements.

a) The validity of the issuer's digital signature should be verified;