

ICS 35.100
CCS L 79



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

GB/Z 185.3-2026

**Artificial intelligence - Agent interconnection - Part 3: Identity
management**

人工智能 智能体互联 第3部分：身份管理

Issued on: May 22, 2026

Implemented on: May 22, 2026

**Issued by: State Administration for Market Regulation;
Standardization Administration of China**

Table of Contents

- 3 Identity Management Released on 2026-05-
- 6 Identity Registration and Verification
- 7 Identity Account Management
- 8 Voucher Management
- 9 Identity Verification

Foreword

GB/Z 185.3-2026: Artificial intelligence - Agent interconnection - Part 3: Identity management

GB /Z 185.3-2026. Interconnection of Intelligent Agents through Artificial Intelligence - Part

3. Identity Management GB /Z 185.3-2026 English version. Artificial intelligence - Agent interconnection - Part

3. Identity management National Standardization Guiding Technical Documents of the People's Republic of China ICS 35.100CCS L 79 AI-powered intelligent agent interconnection Part

3 Identity Management Released on 2026-05-

22 State Administration for Market Regulation The State Administration for Standardization issued a statement.

1. Scope This document specifies the framework and requirements for identity management of intelligent agents in interconnected environments, covering intelligent agent identity registration and verification, identity... Account management, credential management, identity verification, etc. This document applies to the development, application, and evaluation of intelligent agent identity management functions/systems.

4. Abbreviations The following abbreviations apply to this document. HSM. Hardware Security Module TEE. Trusted Execution Environment

5. Intelligent Agent Identity Management Framework The intelligent agent identity management framework is shown in Figure 1. The framework includes the following main roles. --The agent entrusting party. entrusts and authorizes an intelligent agent to carry out activities on its behalf in specific business scenarios, and assumes responsibility for the actions of the intelligent agent. Ultimately, the responsibility usually falls on the human user or the organization. --Intelligent Agent. Accepts authorization from the principal agent and

acts on behalf of the principal agent to carry out activities, and maintains and manages its own identity information. Information, including smart agent identity code and smart agent credentials, etc. --Tool provider. When an agent initiates a protocol-based access request to the tool, the provider authenticates the agent's identity and relies on... The system provides tools and services for identity verification results and access control management for intelligent agents. It also includes a complete set of tools for intelligent agent invocation. The service can be referenced in GB /Z 185.7-2026. --Intelligent agent identity registration service provider. In identity registration and verification, it processes intelligent agent identity registration requests and executes intelligent agent identity verification. The verification process involves creating an identity account for the agent and assigning a corresponding agent identity code and issuing agent credentials upon successful verification. After completing the registration of the agent's identity, maintain and manage the agent's identity account. --Agent credential issuer. Responsible for generating, issuing, and managing agent credentials. This party can be involved in agent identity registration. The service provider can belong to the same organization, or it can be an independent third-party organization. --Agent authentication party. During the identity authentication process, it is responsible for verifying the authenticity and completeness of the agent credentials presented by the agent. And validity. During the verification process, the agent's identity verification party may interact with the agent's credential issuer to complete the verification. Validation of agent credentials. The framework includes the following main processes. --Agent identity management can be further divided into. - Identity Registration and Verification. This activity describes the process of registering the identity of an agent, that is, creating an identity for the agent. The prerequisites for subsequent intelligent agent identity management and applications are detailed in Chapter 6; - Identity and Account Management. This activity describes the process of managing the identity and account of an agent, including identity updates and identity locks. For details on locking, unlocking, and identity cancellation, please refer to Chapter 7. --Credential Management. This activity describes the process of issuing and managing agent credentials associated with an agent's identity, including credential management. This includes certificate issuance, certificate renewal, certificate locking and unlocking, and certificate cancellation. This is in addition to issuance through smart agent identity registration service providers. In addition to managing agent credentials, agents can also directly apply for and manage agent credentials from the issuer of the agent credentials. See Chapter 8. --Identity Authentication. This activity describes how an agent proves its identity to other entities, including in scenarios involving agent interactions and... Scenarios for tool access, etc. See Chapter 9.

Note. In Figure 1, when agent A initiates an interaction request to agent B, agent B verifies agent A's identity and proceeds accordingly based on the verification result. Subsequent interconnection authentication is performed to determine whether to accept the interaction request from agent A and provide corresponding services or resources.

6 Identity Registration and Verification

6.1 General Process The general process for agent identity registration and verification is as follows:

- a) Identity Registration Initiation. After authorizing the agent, the agent's principal initiates the registration process with the agent's identity registration service provider. The registration request submits registration information about the agent, such as a description of the agent's functions, a list of supported tasks, and the version. Number, etc.;
- b) Risk Assessment and Evidence Requirements. The agent identity registration service provider analyzes the received registration information, assesses its potential risks, and The combination of identity verification documents required for this registration will be determined based on the assessment results.
- c) Identity Evidence Submission and Verification. The agent identity registration service provider collects the necessary evidence from multiple sources, including the agent's client and the agent itself. Required supporting documents, and verification and validation of the supporting documents;
- d) Identity Establishment and Credential Issuance. After identity verification is successful, the agent identity registration service provider creates an identity account for the agent. The system identifies users and assigns them intelligent agent identity codes, which can be done according to GB /Z 185.2-2026. Simultaneously, it assigns identity codes to the intelligent agent credential issuer. Initiate a request to generate the corresponding agent credentials for the agent;
- e) Identity Account Activation. The agent identity registration service provider returns the agent identity code and associated agent credentials to the agent. The agent's identity account will be activated at that time to complete the identity registration and verification process.

Note. For details on the implementation of identity registration, verification, and credential issuance, please refer to Appendix A.

6.2 Identity verification documents Supporting documents that can be used for agent identity verification include, but are not limited to. supporting documents related to system structure and authorization documents. Documents, supporting evidence of the boundaries of behavior, and other supporting materials.

Note. See Appendix B for specific example materials.

7 Identity Account Management

7.1 General Rules Identity account management is as follows:

- a) The intelligent agent identity registration service provider should support processes such as identity registration, identity update, and identity cancellation;
- b) The intelligent agent identity registration service provider should support processes such as identity locking and identity unlocking;
- c) The intelligent agent identity registration service provider should formulate clear rules to define whether an identity update is triggered when an intelligent agent changes or whether it is treated as a new identity. The agent is re-registered.

7.2 Identity Update Regarding identity updates.

- a) The intelligent agent identity registration service provider should support identity update processes initiated by the intelligent agent, and the process should preferably include the intelligent agent's principal. Confirmation information;
- b) During the identity update process, the agent's identity code should remain unchanged;
- c) Any update operation to an identity account should be subject to appropriate authorization and authentication, and corresponding log records should be generated, with technical measures in place to prevent [further issues]. Prevent unauthorized modification of logs;
- d) Intelligent agents should support identity update processes initiated proactively by the intelligent agent identity registration service provider;
- e) When the agent changes (e.g., changes occur in core code, function list, permission scope, runtime environment, etc.), the agent should issue a warning. Start the identity update process.

7.3 Identity Locking and Unlocking Regarding identity locking and unlocking.

- a) When an identity account is locked, the agent identity registration service provider and the agent credential issuer should refuse to interact with that account. For related requests such as voucher issuance and voucher updates, the voucher should be considered invalid during verification;
- b) Locking and unlocking operations on identity accounts should be subject to appropriate authorization and authentication, generate corresponding log records, and employ technical measures to prevent [illegal activities]. Prevent unauthorized modification of logs;
- c) The intelligent agent identity registration service provider should support identity locking and unlocking processes initiated by the intelligent agent, and the process should include intelligent agent identification features. Confirmation information from the client who commissioned the energy source;

8 Voucher Management