

ICS 35.030
CCS L 80



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

GB/T 47690-2026

**Cybersecurity technology - Public service for national network
identity authentication - Requirements for application access**

网络安全技术 国家网络身份认证公共服务 应用接入要求

Issued on: May 25, 2026

Implemented on: December 1, 2026

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

Table of Contents

- 1 Scope
- 5 Overview
- 6 Access Requirements

Foreword

GB/T 47690-2026 | Cybersecurity technology - Public service for national network identity authentication - Requirements for application access

GB/T 47690-2026 English version. Cybersecurity technology - Public service for national network identity authentication - Requirements for application access ICS

80 National Standards of the People's Republic of China National Network Identity Authentication Technology for Cybersecurity Public service application access requirements
Published on 2026-05-

25 Implemented on December 1, 2026 State Administration for Market Regulation The State Administration for Standardization issued a statement.

1.Scope This document establishes the overall framework and access methods for the application access of the National Network Identity Authentication Public Service Platform, and proposes supporting application access... The software controls specified the requirements for application access. This document applies to application access to the National Network Identity Authentication Public Service Platform.

4.Abbreviations The following abbreviations apply to this document. APP. Application.

1 Scope

GB/T 47690-2026 is the Chinese national standard covering how an application connects to China's national network identity authentication service - the registration of the application, the authentication flows, the data it may request and retain, and the security obligations that come with being trusted to identify a citizen. First edition, in force from 1 December 2026. It was issued on 25 May 2026 and takes effect on 1 December 2026, as a first edition. The document is under the responsibility of the Standardization Administration of China. 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 Access Institution An access provider is an organization that owns or operates the

access application.

- a) The public service platform supports access from various types of organizations, including government agencies, public institutions, social organizations, and enterprises;
- b) An access institution may apply for access application integration.

5.3 Accessing Application Clients The public service platform supports access from various application clients, including apps, mini-programs, web pages, and application terminals, and supports Android, iOS, and iOS. Examples of QR codes displayed on application clients for various operating systems such as HarmonyOS are shown in Appendix A.

5.4 Network Access The public service platform supports access from various network types, including the Internet, government extranet, and dedicated lines.

5.5 Secure Connection Method Secure connection methods between access applications and public service platforms include secure access device connection and secure access platform connection.

a) **Secure Access Device Connection Method.** Access applications connect to the public service platform through secure access devices. Secure access devices output... The equipment certificate issued by the public service platform is installed at the factory. The access organization deploys secure access equipment and submits it online to the public service platform. Apply for and install the institution's certificate. Establish secure and reliable business access between the access application and the public service platform through secure access devices. Ask about the passage.

b) **Secure Access Platform Connection Method.** Access applications connect to the public service platform through a secure access platform. Access institutions provide services to the public service platform... The service platform applies for organization certificates online and installs them on the secure access platform. The secure access platform can also install public service platforms. Multiple certificates issued by various organizations. Through the relevant interfaces provided by the secure access platform, an agreement is established between the access application and the secure access platform. Establish a secure and reliable business access channel; through secure access devices, the secure access platform and the public service platform establish a secure and reliable connection. The business access channel.

5.6 Supporting Controls The following support controls can be used when integrating applications.

- a) **Face liveness image acquisition control.** can be integrated into the access application client, enabling liveness detection, image quality assessment, encryption, and signature. Facial images meeting the requirements were collected through methods such as...
- b) **Identity Information Security Collection Control.** Can be integrated into the access

application client to collect identity information through encryption, signature, and other methods. Safety at the time;

c) National Network Identity Authentication Client Call Control. Can be integrated into the access application client and interact with the national network identity authentication client. Line interaction.

5 Overview

5.1 Overall Framework for Application Access The National Online Identity Authentication Public Service Platform refers to a platform uniformly constructed by the state based on legal identity document information, providing natural persons with services for applying for online identity authentication. Information systems that provide services such as issuing network numbers and network certificates, and verifying identities. Access Institution Application System (hereinafter referred to as "Access Application") and National Network Identity Authentication Public Service Platform (hereinafter referred to as "Public Service") The platform's docking framework is shown in Figure 1. The application consists of two parts. the server and the client. The public service platform implements application access and management through an application access management system and an application security management system. Among these, application access... The management system is responsible for authorizing and managing access institutions and applications, while the application security management system is responsible for authenticating access institutions and applications. And certificate management. Access applications connect to the public service platform through secure access devices or secure access platforms.

Figure

6 Access Requirements

6.1 Basic Requirements for Access Applications Applications should meet the following basic requirements.

- a) In the National Internet Infrastructure Management System (ICP/IP Address/Domain Name Information Filing Management System) and the National Internet Security Management System Registration of management service platforms, etc.;
- b) Provide the name of the access organization, its unified social credit code, and relevant qualification certificates;
- c) Provide information such as the name and type of the application being accessed, as well as relevant supporting documents;
- d) Define the application scenario and assess the service volume (total daily authentication volume, concurrency);
- e) Changes in the main body of the access institution, the name of the access institution,

the name of the access application, the operational relationship of the access application, the application scenario, and the service volume. When changes occur, the public service platform will be notified to make adjustments.

f) Use within the scope of the application requirements, and do not provide services to third parties.

6.2 Access Application Technical Requirements The application should meet the following technical requirements.

a) Connecting to the public service platform via secure access devices or secure access platforms;

b) Conduct joint testing and release according to the relevant technical interface requirements of the public service platform;

c) Use facial liveness image acquisition controls and identity information security acquisition controls that meet the technical requirements of the public service platform;

d) Meets the relevant technical requirements in GB/T 42573.

6.3 Security Requirements for Access Applications Access application security should meet the following security requirements.

a) Security protection is implemented in accordance with the requirements for network security level protection, meeting the requirements for Level 2 security protection capability as per GB/T 22239. Require;