

ICS 35.030

GM

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

GM/T 0113-2021

Fast online identity authentication protocol

在线快捷身份鉴别协议

(English Translation)

Issued on: October 18, 2021

Implemented on: May 1, 2022

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative references	2
Terms and definitions	3
Abbreviations	4
Overview	5
Registration	6
Overview	7
Extensions	8
Final challenge parameters	9
Protocol messages	10
Rules for the authentication server to generate deregistration request	11
Rules for the biometric key manager to process logout requests	12
Overview	13
Registration	14
Overview	15
Request message framework	16
Short encoding	17
Extended length encoding	18
Rules for the identity authentication server to call registration interface	19
Overview	20
Registration	21
Overview	22
Request message framework	23
Short encoding	24
Extended length encoding	25
Rules for the identity authentication server to call registration interface	26

1 Scope

This document specifies the online fast identity authentication protocol, including the general online fast identity authentication protocol and the two-factor online fast identity authentication protocol.

This document is applicable to the development, testing, evaluation of online fast identity authentication services.

2 Normative references

The contents of the following documents constitute the essential terms of this document through normative references in the text. Among them, for dated references, only the version corresponding to that date applies to this document; for undated references, the latest version (including all amendments) applies to this document.

GB/T 16262 (all parts) Information technology - Abstract syntax notation one (ASN.1) GB/T 16649.4 Identification Cards - Integrated circuit cards - Part 4: Organization, security and commands for interchange GB/T 25069 Information security techniques - Terminology GB/T 32905 Information security techniques - SM3 cryptographic hash algorithm GB/T 32918 (all parts) Information security technology - Public key cryptographic algorithm SM2 based on elliptic curves GB/T 35276 Information security technology - SM2 cryptography algorithm usage specification

3 Terms and definitions

The terms and definitions as defined in GB/T 25069, GB/T 36651, GM/Z 4001, as well as the following terms and definitions, apply to this document.

Authentication client A software component that processes two-factor authentication protocol messages in a user agent, which is used for communication between the user agent and the authenticator in the two-factor authentication protocol.

Authentication client interface A protocol interface provided by the authentication client, which is used for communication between the user agent and the authentication client in the two-factor authentication protocol.

4 Abbreviations

The following abbreviations apply to this document.

APDU. Application Protocol Data Unit AppID. Application Identifier ASN.1. Abstract Syntax Notation One BAP. Biometric Authentication Protocol BAPV. Biometric Authentication Protocol Version

5.1.1 Overview

The General Online Quick Identity Authentication Protocol uses smart devices and combines biometric identification technology, to provide a password-free, highly secure, easy-to-use identity authentication solution.

5.1.2 Registration

In the process of user registration with the identity authentication server, the user uses the biometric key manager to create a new pair of authentication public and private keys;
saves the authentication private key in the biometric key manager;

5.2.1 Overview

All data formats of the general online quick identity authentication protocol are described in GB/T 16262.

5.2.4 Extensions

This structure describes a common extension used in various operations.

id. The identifier of the extension.

5.2.6 Final challenge parameters

applD. The parameter value is set to the applD parameter value of the operation header.

challenge. This parameter value is set to the server challenge parameter value in the registration request or authentication request. The server challenge is a random parameter value provided by the server.

5.2.12 Protocol messages

Protocol messages are messages transmitted by various participants of the general online fast identity authentication protocol when they interact. ASN.1 describes them as follows.

5.3.3.2.1 Rules for the authentication server to generate deregistration request

The authentication server shall follow the following steps.

5.3.3.2.2 Rules for the biometric key manager to process logout requests

The biometric key manager shall follow the following steps.

6.1.1 Overview

For the relying party that has deployed the user authentication method using username/password, the two-factor online fast identity authentication protocol uses the authenticator as the second factor of user identity authentication, to improve the security of user identity authentication.

6.1.2 Registration

When the user registers with the relying party, the authenticator generates a pair of authentication public-private key pairs and sends the authentication public key to the relying party. The relying party saves the authentication public key and binds it to the user's identity, to complete the registration process. The session flow (registration flow) is shown in Figure 6, which uses HTTP redirection to illustrate the protocol interaction.

6.2.1 Overview

The two-factor online quick identity authentication protocol mainly includes request messages and response messages. The request message is created by the authentication client and processed by the authenticator; the response message is created by the authenticator and used by the relying party. This document specifies the encoding method of the request and response messages.

6.2.2.1 Request message framework

The request message is encapsulated as a command APDU; the encapsulation method is as follows.

6.2.2.1.1 Short encoding

In short encoding, the maximum length of request data is 255 bytes. Among them, Lc is encoded as follows.

6.2.2.1.2 Extended length encoding

In extended length encoding, the maximum length of request data is 65535 bytes.

Among them, Lc is encoded as follows.

6.3.1.2.1 Rules for the identity authentication server to call registration interface

The identity authentication server shall follow the following steps to call the registration interface.

Appendix A

(Informative)

Security risks and recommended measures A.1 Malicious relying party an attacker may pretend to be a legitimate relying party. After obtaining the user's private information, the attacker can pretend to be the user and register the authenticator with the real relying party as the user.

The relying party needs to strengthen the identity authentication during registration and the