

ICS 35.040

GM

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

GM/T 0069-2019

Open identity authentication framework

开放的身份鉴别框架

(English Translation)

Issued on: July 12, 2019

Implemented on: July 12, 2019

Issued by: State Administration of Cryptography

Table of Contents

Foreword	1
Scope	2
Normative references	3
Public - key encryption algorithm	4
Overview	5
Overview	6
Requirements for security management user information	7
Requirements for security configuration protocol	8
Requirements for secure transmission and processing of protocol	9
Identification process type	10
Overview	11
Authorization code process steps	12
Authentication request	13
Authentication request validation	14
Authentication success response	15
Overview	16
ID token	17
Overview	18
Encrypted JSON token	19
Overview	20
Normal claim	21
User information successful response	22
Foreword	23
Overview	24
Normal claim	25
User information successful response	26

Foreword

This standard was drafted in accordance with the rules given in GB/T 1.1-2009.

This standard was proposed by and shall be under the jurisdiction of the Cryptographic Industry Standardization Technical Committee.

Drafting organizations of this standard. Data and Communication Protection Research and Education Center of Chinese Academy of Sciences, Beijing Digital Certification Co., Ltd., China Electronics Standardization Institute, Institute of Software of Chinese Academy of Sciences, Beijing Tianrongxin Technology Co., Ltd.

1 Scope

This standard specifies the agreement framework for relying parties (network applications or services) to use the authentication function provided by the identity service provider to authenticate end users; defines the requirements of the entities involved in the agreement, the authentication protocol process, the access requirements of user information, as well as the encryption and signature requirements of protocol messages, etc.

This standard applies to the development, testing, evaluation and procurement of user identification services in scenarios where end users access network applications.

2 Normative references

The following documents are essential to the application of this document. For the dated documents, only the versions with the dates indicated are applicable to this document; for the undated documents, only the latest version (including all the amendments) are applicable to this standard.

GB/T 32905-2016 Information security technology SM3 cryptographic hash algorithm GB/T 32907-2016 Information security technology - SM4 block cipher algorithm GB/T 32918.2-2016 Elliptic curve public - Key cryptography - Part 2: Digital signature algorithm GB/T 32918.4-2016 Elliptic curve public - Key cryptography algorithm - Part

4 Public - key encryption algorithm

GM/T 0024-2014 SSL VPN specification GM/T 0068-2019 Open third party resource authorization protocol framework

3 Terms and definitions the following terms and definitions apply to this document.

Access token

The token issued by the authorization server, which is used to prove that an entity has the authority to access protected resources within a specific range.

Authentication request A request for the purpose of authenticating the identity of the end user.

Note: After the identity service provider receives the request sent by the relying party, it authenticates the terminal user.

Authentication code flow an identity authentication process suitable for relying parties with

confidentiality capabilities to authenticate end users.

Authorization endpoint the endpoint on the authorization server used to interact with the end user, which is used to receive the identity credentials and authorization of the end user, meanwhile return the authorization to the relying party.

4 Abbreviations

The following abbreviations apply to this document.

HTTP. Hypertext Transfer Protocol HMAC. Hash-based Message Authentication Code

5 Overview

The identity authentication protocol framework specified in this standard allows the relying party to use the authentication service of the identity service provider to authenticate the end user. After the end user is successfully authenticated, the relying party can obtain the authorized user's identity information from the identity service provider.

6.1.1 Overview

The identity service provider is an entity that provides identity authentication services for end users who access the relying party and shall provide the following functions.

6.1.2 Requirements for security management user information

The identity service provider shall securely manage and store the user's identity information, including the subject identifier, name, avatar, gender, date of birth, email address, mobile phone number, residential address and other identity attributes that identify the user. The type of these attribute information is defined and required by the identity service provider according to service needs (see Appendix A).

6.1.3 Requirements for security configuration protocol

The identity service provider shall provide the necessary basic configuration (see Appendix B) to implement the protocol process. First, the identity service provider shall provide the issuer identifier (usually URI), so that the relying party can find the identity service provider when executing the identity service discovery protocol.

6.1.4 Requirements for secure transmission and processing of protocol

messages

7.1 Identification process type

This standard defines three types of identity authentication processes based on different types of relying parties and different needs. The authentication process is executed by the server of the identity service provider.

7.2.1 Overview

This section describes how to use the authorization code-based authentication process to authenticate the end user.

7.2.2 Authorization code process steps

The authorization code process includes the following steps.

7.2.3.1 Authentication request

The authentication request is constructed by the relying party and used to request the authorization server to authenticate the end user.

7.2.3.2 Authentication request validation

After receiving the request, the authorization server shall perform the following validation.

7.2.3.5 Authentication success response

After the end user successfully passes the identity authentication, the authorization endpoint of the identity service provider shall use the "authentication success response" message as defined in this clause to respond to the authentication request message sent by the relying party.

When using the authorization code authentication process, the authorization server shall send the authorization code to the relying party, usually through redirection. The authorization server adds the following parameters to the query component of the redirection endpoint URI (first use UTF-8 to encode the parameters; then use the "application/x-www-form-urlencoded" [RFC1867] format for encoding).

8.1.1 Overview

The protocol defined in this standard mainly involves three types of tokens. ID tokens, access tokens and refresh tokens.

8.1.2 ID token

The ID token is a JSON token containing the authorization claim of the end user;