

ICS 35.0404

GM

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

GM/T 0068-2019

Open third party resource authorization protocol framework

开放的第三方资源授权协议框架

(English Translation)

Issued on: July 12, 2019

Implemented on: July 12, 2019

Issued by: State Administration of Cryptography

Table of Contents

Scope	1
Normative References	2
Protocol channel requirements	3
Types of third-party applications	4
Third-party application identifier	5
Registration requirements for the third-party applications	6
Authentication scheme of the password credential of the third-party	7
Authorization request	8
Error response	9
Access token	10

1 Scope

This Standard specifies the process of third-party resource authorization protocol, different types of authorization licenses, the functional requirements of each endpoint of the protocol, and the format and parameter requirements of messages transmitted between system entities.

This Standard is applicable to the development, testing, evaluation and procurement of identity authentication and authorization services in the Internet cross-security domain application scenario.

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 document.

GB/T 15843.3-2008 Information Technology - Security Techniques - Entity Authentication - Part 3: Mechanisms Using Digital Signature Techniques
 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 Information Security Technology - Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 2: Digital Signature Algorithm
 GB/T 32918.4-2016 Information Security Technology - Public Key Cryptographic Algorithm SM2 Based on Elliptic Curves - Part 4: Public Key Encryption Algorithm
 GM/T 0024-2014 SSL VPN Specification
 RFC 1867 Form-Based File

Upload in HTML RFC 2616 Hypertext Transfer Protocol - HTTP/1.1 RFC 2617 HTTP Authentication: Basic and Digest Access Authentication party application uses the authorization server as an intermediary to obtain the authorization grant from the resource owner, as shown in Figures 2 and 3;

- b) The resource owner [or the resource owner indirectly through the authorization server, as described in step a)] issues authorization grant to the third-party application. This authorization grant is a credential authorized by the resource owner, and the used type is one of the four types defined in 7.1.1. The type of authorization grant depends on the way the third-party application requests authorization [that is, the two ways described in step a)] and the type of authorization grant supported by the authorization server (usually provided by the service document of the authorization server);
- c) The third-party application authenticates the authorization server and submits the authorization grant, requesting an access token from the authorization server;
- d) The authorization server authenticates the identity of the third-party application and verifies the validity of the authorization grant. If the identity of the third-party application is successfully authenticated and the authorization grant is valid, the authorization server issues an access token to the third-party application;
- e) Third-party applications send access tokens and related parameters to the resource server to request access to protected resources;
- f) The resource server verifies the validity of the access token. If the access token is valid, the requested resource is returned to the third-party application.

Based on the above protocol process, third-party application may interact with the resource owner through the user agent (such as a browser) used by the resource owner. In some specific situations (see 7.5), the third-party application may not interact with the resource owner. Interactively, directly use the identity credentials of the third-party application to obtain the access token issued by the authorization server. If the third-party application's access to the protected resource exceeds the scope or validity period of the access token, the access becomes invalid; and the third-party application should restart the protocol process or use the refresh mechanism specified in this Standard to update the access token.

This Standard uses the hypertext transfer protocol HTTP1.1 (see RFC 2616) for communication. The open third-party resource authorization protocol framework based on any other protocol does not belong to the scope of this Standard.

5.2 Protocol channel requirements

For sensitive data such as authorization codes, access tokens, refresh tokens, resource owner password credentials, and third-party application identity credentials, plaintext

transmission shall not be used; and the secure transport layer protocol defined by GM/T 0024-2014 shall be used for transmission. The authorization server If the third-party application has registered multiple redirection endpoint URIs, or only registered a part of the redirection endpoint URI, or has not registered the redirection endpoint URI, the third-party application shall use < redirect_uri> parameter in the request when sending authorization requests to identify the redirection endpoint URI used in this request.

When the authorization request contains the redirection endpoint URI, if the third-party application has registered the redirection endpoint URI, the authorization server shall use the comparison and matching method defined in section 6 of RFC 3986 to compare and match the received redirection endpoint URI and the previous registered redirection endpoint URI. If the third-party application registers the complete URI, the authorization server shall use the simple string comparison method defined in section 6.2.1 of RFC 3986 to compare the two redirection endpoint URIs.

If the authorization request fails verification because the redirection endpoint URI is missing, invalid, or mismatched, the authorization server shall inform the resource owner of the error, and shall not automatically redirect the user agent to the redirection endpoint URI that fails the verification.

The redirection request sent to the redirection endpoint of the third-party application usually gets the response of the HTML document, and the response is processed by the user agent. The third-party applications shall not include any third-party scripts in the response to the redirection request. The third-party applications shall parse out the credentials from the redirected request URI and redirect the user agent to another endpoint again to avoid exposing the credentials in the URI or elsewhere.

6.1 Types of third-party applications

According to whether the third-party applications have the ability to keep their identity credentials confidential, this Standard defines two types of third-party applications:

a) Confidentiality type the third-party application has the ability to maintain the confidentiality of its credentials (for example, the third-party application runs on a secure server that strictly enforces access control), so that it can prove the authenticity of its identity by providing secure identity credentials; or the third party application has the ability to prove the authenticity of its identity through other methods (not specified in this Standard).

b) Non-confidentiality type Third-party applications are unable to maintain the confidentiality of their application, nor shall be threatened by other applications on the same device.

6.2 Third-party application identifier

The third-party application identification is an application identifier issued by the authorization server for registering the third-party application. This identifier is a string, and the authorization server may use this string to uniquely identify a third-party application.

This Standard does not specify the length of third-party application identifiers. The authorization server shall specify the length of this identifier and make detailed records of any length of identifiers issued by it. The third-party applications shall not make assumptions about the length of this identification.

6.3 Registration requirements for the third-party applications

Before the implementation of the protocol, the provider of the third-party application needs to register the third-party application's information (such as redirection endpoint URI, the third-party application type, etc.) on the authorization server to establish a trust relationship between the third-party application and the authorization server. The third-party application provider shall use the registration method (usually provided by the service document of the authorization server) supported by the authorization server to complete the registration process. The specific registration method does not belong to the scope of this Standard.

When registering a third-party application, the third-party application provider should provide the following information to the authorization server:

- a) The type of third-party application (see 6.1);
- b) Redirection endpoints pointing to third-party applications (see 5.3.4);
- c) Other information required by the authorization server (such as application name, website and description, etc.).

6.4.1.1 Authentication scheme of the password credential of the third-party application

When the authorization server uses the authentication-scheme-based on password credentials to authenticate third-party applications, the authorization server can use the HTTP digest to access authentication scheme (digest access authentication scheme, see RFC 2617). The third-party applications use the SM3 algorithm (see GB/T 32905-2016) to hash the nonce parameter values (random string to prevent replay an identity authentication method that meets the security requirements of the authorization server (usually provided by the service document of the authorization server) shall be established between the confidentiality third-party application and the authorization server; so that the authorization server can securely authenticate the identity of the third-party application. When the authorization server usually registers on the confidentiality third-party application, the identity credentials (such as passwords, digital certificates) shall be granted to the