ICS 35.040
L 80

GM

中华人民共和国密码行业标准

GM/T 0069—2019

开放的身份鉴别框架

Open identity authentication framework

2019-07-12 发布　　2019-07-12 实施

国家密码管理局　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由密码行业标准化技术委员会提出并归口。

本标准起草单位：中国科学院数据与通信保护研究教育中心、北京数字认证股份有限公司、中国电子技术标准化研究院、中国科学院软件研究所、北京天融信科技有限公司。

本标准主要起草人：高能、彭佳、刘泽艺、李敏、钱文飞、江伟玉、刘伟、李向锋、刘丽敏、屠晨阳、张立武、景鸿理、郝春亮。

引　言

互联网环境中，用户使用多个网络应用已经成为常态。身份鉴别技术呈现出开放性、易用性以及互操作性的特点。本标准提出的身份鉴别框架使得网络应用可以便捷地使用身份服务提供方提供的鉴别服务，由身份提供方对用户进行身份鉴别，验证用户的身份，并在用户授权之后可以提供用户身份相关信息。

开放的身份鉴别框架

1 范围

本标准规定了依赖方(网络应用或服务)使用身份服务提供方提供的鉴别功能、对终端用户进行身份鉴别的协议框架,定义了协议参与实体的要求、鉴别协议流程、用户信息的访问要求,以及协议消息的加密和签名要求等。

本标准适用于终端用户访问网络应用的场景中,用户身份鉴别服务的开发、测试、评估和采购。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件,仅注日期的版本适用于本文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 32905—2016 信息安全技术 SM3 密码杂凑算法

GB/T 32907—2016 信息安全技术 SM4 分组密码算法

GB/T 32918.2—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 2 部分:数字签名算法

GB/T 32918.4—2016 信息安全技术 SM2 椭圆曲线公钥密码算法 第 4 部分:公钥加密算法

GM/T 0024—2014 SSL VPN 技术规范

GM/T 0068—2019 开放的第三方资源授权协议框架

ISO 639-1 各种语言中名字的编码表示 第 1 部分:Alpha-2 编码(Codes for the representation of names of languages—Part 1:Alpha-2 code)

ISO 3166-1 各个国家的名字和名字细分的编码表示 第 1 部分:国家编码(Codes for the representation of names of countries and their subdivisions—Part 1:Country codes)

ISO 8601:2004 数据元素与交换格式 信息交换 日期与时间格式(Data elements and interchange formats—Information interchange—Representation of dates and times)

ISO/IEC 29115:2013 信息技术 实体鉴别保障框架(Information technology—Entity authentication assurance framework)

RFC 1867 HTML 中基于表单的文件上传(Form-based File Upload in HTML)

RFC 3966 电话号码的电话 URI(The tel URI for Telephone Numbers)

RFC 3986 统一资源标识符:通用语法(Uniform Resource Identifier (URI):Generic Syntax)

RFC 4627 应用/JSON 的 JavaScript 对象符号的媒体类型(The application/json Media Type for JavaScript Object Notation (JSON))

RFC 5322 互联网信息格式(Internet Message Format)

RFC 5646 语言识别标签(Tags for Identifying Languages)

RFC 6125 基于域的使用网络公钥基础设施(安全传输层协议上下文中使用 X.509 证书)的应用服务标识的表示与验证(Representation and Verification of Domain—Based Application Service Identity within Internet Public Key Infrastructure Using X.509 (PKIX) Certificates in the Context of Transport Layer Security (TLS))

E.164 国际公用电信编号计划(The international public telecommunication numbering plan)

3 术语和定义

下列术语和定义适用于本文件。

3.1

访问令牌 access token

授权服务器发放的令牌，用于证明某实体具有访问特定范围内受保护资源的权限。

3.2

身份鉴别请求 authentication request

以鉴别终端用户身份为目的的请求。

注：身份服务提供方接收到依赖方发送的该请求后，对终端用户进行身份鉴别。

3.3

授权码鉴别流程 authorization code flow

适合于有保密能力的依赖方，用于鉴别终端用户的一种身份鉴别流程。

3.4

授权端点 authorization endpoint

授权服务器上用于与终端用户交互的端点，用于接收终端用户的身份凭据和授权，以及返回授权许可给依赖方。

3.5

授权许可 authorization grant

身份服务提供方发放给依赖方的凭据，表明用户同意依赖方访问其身份信息。依赖方不应使用该凭据直接访问用户身份信息，应使用该凭据从授权服务器换取访问令牌。

3.6

授权请求 authorization request

依赖方发送给身份服务提供方的、以获得终端用户授权为目的的请求。

3.7

授权服务器 authorization server

对依赖方进行授权的服务器，一般有两个功能接口：授权端点和令牌端点。

3.8

声明 claim

由身份服务提供方生成的关于实体的数据，包括与实体相关的身份属性或鉴别结果。

3.9

声明类型 claim type

用于表述声明值的语法。本标准定义了规范性(Normal)、聚合式(Aggregated)和分布式(Distributed)三种声明类型。

3.10

凭据 credential

一种凭证，拥有该凭证的实体可以使用该凭证关联的资源。

3.11

端点 endpoint

身份服务提供方用于接收请求消息、返回响应消息的接口。

3.12

终端用户　end-user

使用信息系统和系统资源的自然人。

3.13

混合鉴别流程　hybrid flow

一种结合授权码鉴别流程和隐式鉴别流程的混合流程。

3.14

标识符　identifier

在特定上下文中唯一标识一个实体的字符串。

3.15

身份　identity

实体的属性信息集合。

3.16

身份服务提供方　identity service provider

向依赖方提供关于用户身份鉴别结果及相关授权的实体，鉴别终端用户，并为依赖方提供关于用户身份鉴别结果的声明。

3.17

ID 令牌　ID token

包含关于终端用户身份鉴别结果的声明，还可能包含一些其他声明。

3.18

隐式鉴别流程　implicit flow

适于无保密能力的依赖方使用的、用于鉴别终端用户的一种身份鉴别流程。

3.19

发布方　issuer

发布声明的实体。

3.20

发布方标识符　issuer identifier

用来识别发布方的标识符。

注：发布方标识符是大小写敏感的 URL，使用 HTTPS 机制包含模式、主机，并可选端口号和路径，但不包括查询部分和片段部分。

3.21

个人身份信息　personally identifiable information；PII

用于识别某个自然人身份的信息，或是关联到某个自然人的相关信息。

3.22

依赖方　relying party

依赖于身份服务提供方对访问它的终端用户进行鉴别的实体。

3.23

主体标识符　subject identifier

身份服务提供方发放给终端用户的、用于标识终端用户身份的标识符。

注：该标识符在身份服务提供方唯一存在且不再次发放，由依赖方使用。

3.24

令牌端点　token endpoint

授权服务器上用于与依赖方交互的端点，授权服务器使用该端点接收依赖方发起的令牌请求，当授

权服务器验证请求成功后，通过该端口返回令牌给依赖方。

3.25

用户信息端点　userinfo endpoint

身份服务提供方用于接收访问和返回受保护的用户信息的功能接口。

注：依赖方向该端点呈递访问令牌时，该端点将根据终端用户的授权返回有关终端用户的授权信息。用户信息端点的 URL 应使用 HTTPS 机制，并可能包含端口、路径和查询部分。

3.26

验证　validation

核验符合某种结构的信息具备合理性和正确性的过程。

4　缩略语

下列缩略语适用于本文件。

HTTP　超文本传输协议(Hypertext Transfer Protocol)

HMAC　基于杂凑的消息鉴别码(Hash-based Message Authentication Code)

TLS　安全传输层协议(Transport Layer Security)

URI　统一资源标识(Uniform Resource Identifier)

URL　统一资源定位符(Uniform Resource Locator)

5　概述

本标准规范的身份鉴别协议框架，使得依赖方可以利用身份服务提供方的鉴别服务对终端用户进行鉴别。终端用户成功通过鉴别之后，依赖方可以从身份服务提供方获得经过授权的用户身份信息。

本标准规范的身份鉴别协议框架主要涉及三类参与实体：依赖方、身份服务提供方和终端用户。本标准主要对依赖方和身份服务提供方的功能进行规定：

——依赖方：依赖方被终端用户访问时，依赖方应对终端用户进行身份鉴别。对于尚未鉴别的终端用户，依赖方选择某身份服务提供方对终端用户进行身份鉴别；

——身份服务提供方：对终端用户进行鉴别，并向鉴别成功的终端用户，询问关于依赖方访问用户身份信息的授权，得到终端用户授权后，最终将授权后的用户身份信息发送给依赖方，完成身份鉴别。其中，身份服务提供方的授权服务器实现对终端用户身份的鉴别，授权服务器包含两个功能接口：授权端点和令牌端点；身份服务提供方通过提供用户信息端点，实现依赖方对用户信息的访问功能。

端点使用 URI 进行标识。URI 的典型格式是：[方案(scheme)：][//主机名(authority)][路径(path)][？查询组件(query)][＃片段组件(fragment)]，查询组件和片段组件的编码格式应为“application/x-www-form-urlencoded”(见 RFC 1867)编码格式。

依赖方、身份服务提供方和终端用户等三者之间的交互均应采用密码技术来保障安全，且依赖方和身份服务提供方均应进行相关的配置来支持协议，本标准规范了依赖方和身份服务提供方的实体要求(见第 6 章)。

当终端用户访问依赖方提供的服务时，如果依赖方要求对终端用户进行鉴别且支持本标准定义的协议，依赖方可将终端用户重定向到该依赖方信任的身份服务提供方，执行以下协议流程(见图 1)：

a)　鉴别请求：依赖方向身份服务提供方发送关于终端用户的鉴别请求；

b)　鉴别与授权：身份服务提供方的授权端点鉴别终端用户，并向终端用户获取关于依赖方访问其

数据的授权；

c） 鉴别响应：身份服务提供方的令牌端点（或授权端点）返回 ID 令牌，通常还会返回访问令牌，从而响应第 a）步的请求；

d） 用户信息请求：依赖方发送带有访问令牌的请求到身份服务提供方的用户信息端点；

e） 用户信息响应：用户信息端点返回关于终端用户的身份信息。

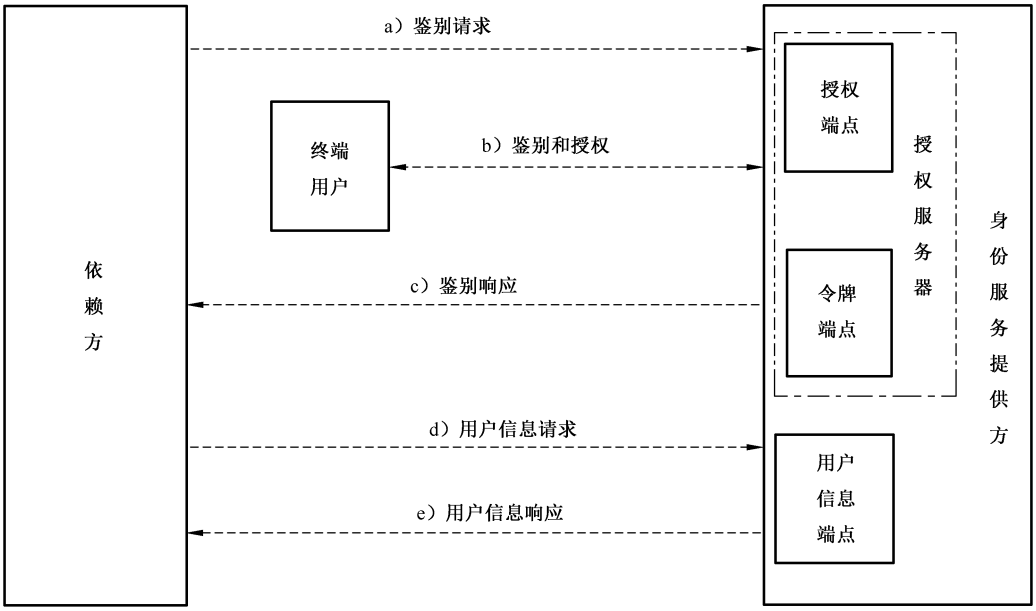

图 1 身份鉴别协议框架

依赖方的类型不同，具备的对机密信息的保密能力不同，所使用的身份鉴别协议流程也会产生差异。本标准定义并规定了三种身份鉴别流程，分别是授权码鉴别流程、隐式鉴别流程和混合鉴别流程。

本标准规范的身份鉴别协议，使用安全令牌来保护用户敏感信息的传输和访问安全。通过使用安全令牌，可避免将终端用户的身份凭证共享给依赖方，并能将终端用户的身份信息安全地呈递给依赖方。为了确保令牌的安全及其使用安全，本标准定义并给出了令牌的安全要求。

在依赖方呈递访问令牌给身份服务提供方以及获取用户信息的过程中，本标准给出了具体的使用令牌访问用户身份信息的定义和要求，主要涉及协议中传输的关于实体的声明以及用户信息端点要求等。

最后，本标准给出了保障协议安全的签名和加密要求。

此外，本标准也支持一些不常用的身份鉴别发起方式。通常情况下，身份鉴别服务由依赖方向身份服务提供方发起。但在某些情况下，身份鉴别可能由身份服务提供方或其他实体发起。例如，正在使用身份服务提供方 A 的用户通过 A 的页面的链接访问应用 B（依赖方）的购物页面，A 直接向未经过鉴别的用户发起身份鉴别流程，这种情况下，身份鉴别不由依赖方 B 直接发起。另外，一般情况下，用户信息的访问需要终端用户的实时授权，在获得用户授权后，依赖方才可以获得被授权的用户信息。本标准也支持终端用户离线时的用户信息访问，不需要用户在线实时授权。例如，终端用户可以在身份服务提供方进行预先授权，配置依赖方的访问权限，从而使得依赖方在向身份服务提供方请求用户信息时，不需要用户在线进行实时授权。但是，对于用户离线的用户信息访问，由于存在安全风险，应慎重使用。

6 实体要求

6.1 身份服务提供方要求

6.1.1 概述

身份服务提供方是为访问依赖方的终端用户提供身份鉴别服务的实体，应提供以下功能：

a) 安全管理用户信息：管理和安全存储用户身份属性，使用内部唯一的主体标识符标识终端用户；

b) 安全配置协议接口、参数：配置协议执行需要的接口、URL 地址、加解密参数、响应参数等，以能被依赖方发现，并能安全执行协议；

c) 安全传输和处理协议消息：安全接收和处理来自依赖方或者其他实体发起的实体身份鉴别请求；

d) 鉴别和授权：鉴别终端用户，获取终端用户授权，并能够根据终端用户的授权，提供授权范围内的终端用户身份信息给依赖方。

6.1.2 安全管理用户信息要求

身份服务提供方应安全地管理和存储用户的身份信息，包括标识用户的主体标识符、名称、头像、性别、出生年月、邮箱地址、手机号、住址等各类身份属性，这些属性信息的类型由身份服务提供方根据服务需要进行定义和要求(见附录 A)。

身份服务提供方应为终端用户分配唯一且永不被重新分配的主体标识符，以标识终端用户。本标准支持两类主体标识符：公共标识符类型和成对标识符类型：

——〈public〉参数，公共标识符使用该参数描述，若使用该类型，则同一终端用户在所有的依赖方都使用相同的主体标识符；

——〈pairwise〉参数，成对标识符使用该参数描述，若使用该类型，则同一终端用户在不同的依赖方使用不同的主体标识符，以防止依赖方未经许可关联终端用户在其他依赖方的活动。

另外，身份服务提供方应给其终端用户提供用户信息的访问日志，以便终端用户可以对用户信息的访问情况进行监控。

6.1.3 安全配置协议要求

身份服务提供方应提供必要的基础配置(参见附录 B)以实现协议流程。首先，身份服务提供方应提供发布方标识符(通常是 URI)，以便依赖方在执行身份服务发现协议时，找到身份服务提供方。其次，应配置和提供授权端点的 URI、令牌端点的 URI、加密和签名令牌的密钥的 URI、响应类型、响应参数等信息，并提供依赖方应了解的配置信息的方法。本标准假定依赖方已经获得了身份服务提供方的配置信息，依赖方可以通过自动发现过程或者其他方式获得这些信息，本标准不对具体的自动发现过程或其他发现身份服务的方式进行规定。

其中，发布方标识符是用于标识身份服务提供方的标识符。本标准支持多个发布方，每个主机和端口的组合为一个发布方，多个主机和端口的组合可实现多个发布方。一般情况下，本标准要求每台主机仅支持一个发布方。但是，如果该主机支持多个租户，可能需要支持多个发布方。

通过发现过程返回的发布方标识符应与 ID 令牌(见 8.1.2)的〈iss〉参数值完全匹配。发布方标识符应与用户的主体标识符完全对应，即使两个终端用户的主体名相同，但发布方标识符不同，则应视为两个不同的用户。

6.1.4 安全传输和处理协议消息要求

身份服务提供方应提供安全的身份鉴别方法使得：依赖方可对身份服务提供方进行身份鉴别，从而防止恶意的服务器伪装成合法的服务器；对于具有保密能力的依赖方，身份服务提供方应提供鉴别依赖方的方法，从而防止恶意的依赖方假冒合法的依赖方获取用户信息。

身份服务提供方应与依赖方建立安全的会话，应使用 SSLVPN 技术规范 GM/T 0024—2014 中定义的安全通信协议进行通信。

在与依赖方建立安全连接的过程中，身份服务提供方应将其完整域名与其公钥进行绑定，以便依赖方可以验证。本标准还提供了一种利用国产密码算法实现的签名 JSON 令牌或加密 JSON 令牌的方式来实现身份鉴别(见 8.2)。

一般情况下，身份服务提供方应使用非自签名的证书来实现 ID 令牌、访问令牌等安全凭据的签名。本标准也支持自颁发证书的身份服务提供方，使用自颁发证书的身份服务提供方，应进行特殊的参数配置，本标准不作具体规定。

6.1.5 鉴别与授权要求

身份服务提供方应提供安全的鉴别方法对终端用户的身份进行鉴别。例如，用户名/口令方式，数字证书，用户名/智能密码钥匙(USB Key)方式，多因素鉴别方式或其他鉴别方式。本标准不对具体的鉴别方法进行规定。

身份服务提供方在将终端用户的身份信息发送给依赖方之前，应获得终端用户的授权，仅能将用户授权范围内的用户信息发送给依赖方，并能采用安全的访问控制机制，防止非授权的访问。

6.2 依赖方要求

6.2.1 概述

依赖方是使用身份服务提供方对访问它的终端用户进行鉴别的实体。依赖方的类型不同，本标准对依赖方的要求也不同，其所适合的鉴别流程也不相同。本标准定义了两类依赖方。同时本标准还规定依赖方应具备以下功能：

a) 注册和协议配置：向身份服务提供方进行注册，提供协议正常执行需要的参数信息，以便身份服务提供方能够与依赖方建立安全会话，执行协议流程；

b) 依赖方身份鉴别：向身份服务提供方进行身份鉴别，提供支持的身份鉴别方法，以防止恶意的依赖方假冒合法的依赖方。

6.2.2 依赖方的类型

根据依赖方是否对其身份凭据具有保密能力，本标准定义了两种依赖方类型：

a) 有保密能力型

依赖方有能力维持其凭据的机密性(例如，依赖方应用程序运行在严格执行访问控制的安全服务器上)，从而可通过提供安全的身份凭据来证明自己身份的真实性，或者依赖方有能力通过其他的方式(超出本标准的范围)证明自己身份的真实性。

b) 无保密能力型

依赖方没有能力维持其凭据的机密性(例如，依赖方程序运行在资源拥有者使用的设备上，本地应用或是基于浏览器的应用等)，无法提供安全的身份凭据来证明自己身份的真实性，并且没有能力通过其他方式证明自己身份的真实性。

依赖方类型的认定取决于身份服务提供方的鉴别安全要求和对依赖方凭据暴露级别的接受程度

(通常由身份服务提供方的服务文档提供)。授权服务器不应对依赖方的类型进行假定。

6.2.3 依赖方注册和协议配置要求

依赖方在使用身份服务提供方的身份鉴别服务时,应向身份服务提供方注册必要的协议参数,例如,提供用于接收消息的重定向 URL 地址、主页 URL 地址、联系方式、依赖方类型、支持的鉴别依赖方身份的方法等信息(参见附录 C 所描述的注册信息)。

在注册成功时,依赖方会从身份服务提供方获得以下表示身份凭证的参数值对,以用于依赖方身份鉴别:

a) 〈client_id〉依赖方的标识符;

b) 〈client_secret〉依赖方的口令。

6.2.4 依赖方身份鉴别要求

当身份服务提供方使用令牌端点与依赖方进行交互时,依赖方应使用某种鉴别方法向身份服务提供方进行身份鉴别。在依赖方注册时,依赖方应通过下述参数值注册一种依赖方身份鉴别的方法:

a) client_secret_basic

表示已经从身份服务提供方收到了〈client_secret〉值的依赖方,使用 HTTP 基本身份验证方案向身份服务提供方进行身份鉴别。如果依赖方没有注册任何方法,则默认方法是 client_secret_basic 表示的方法;

b) client_secret_post

表示已经从身份服务提供方收到了〈client_secret〉的依赖方,通过在请求主体中包含依赖方凭据的方式向身份服务提供方进行身份鉴别;

c) client_secret_jwt

表示已经从授权服务器收到了〈client_secret〉的依赖方,使用 HMAC SM3 算法创建 JSON 令牌,其中 HMAC SM3 表示基于杂凑算法 SM3(见 GB/T 32905—2016)实现消息鉴别码。HMAC 使用 client_secret 的 UTF-8 编码表示的八位位组作为共享密钥进行计算。

不在令牌端点执行鉴别的依赖方,可能因为它仅使用隐式鉴别流程(所以不使用令牌端点,见 7.3),或者因为它是无保密能力型依赖方,没有保护密钥的能力或不支持其他身份鉴别机制。

7 鉴别流程

7.1 鉴别流程类型

本标准根据依赖方类型的不同及需求的不同,定义了三种身份鉴别流程。鉴别流程由身份服务提供方的服务器执行,该服务器以安全的通信方式返回鉴别结果给依赖方,从而使得依赖方能够根据该结果进行后续的用户信息访问流程。其中,鉴别结果由 ID 令牌(见 8.1.2)返回,包含以下声明的信息:发布方标识符、主体标识符、鉴别有效期等。

三种身份鉴别类型:

——授权码鉴别流程。适用于有能力维持其凭据机密性的依赖方,例如,具有后台 Web 服务器的依赖方,此类依赖方可使用该流程进行终端用户身份的鉴别。在与令牌端点交互时,身份服务提供方可对依赖方进行身份鉴别。所有令牌从身份服务提供方的令牌端点返回,令牌不透漏给用户代理。依赖方获得访问令牌和刷新令牌后,可以进行后续的访问令牌刷新流程。

——隐式鉴别流程。适用于无能力维持其凭据机密性的依赖方,例如运行在浏览器上的 JS 代码或本地应用程序,此类依赖方可使用该流程进行终端用户身份的鉴别。依赖方不与令牌端点进行交互,也不进行依赖方身份鉴别,不可进行后续的令牌刷新流程。所有的令牌从身份服务提

供方的授权端点返回。

——混合鉴别流程。结合了前两种鉴别流程。该流程适用于此类依赖方：依赖方应用程序能够通过立即使用 ID 令牌获得终端用户的身份，并且（如其后台服务程序）能够通过使用授权码，请求刷新令牌以获得更长期的访问权限。在与令牌端点交互时，身份服务提供方可对依赖方进行身份鉴别。使用该流程时，部分令牌从身份服务提供方的授权端点返回，部分令牌从令牌端点返回。依赖方获得刷新令牌后，可以进行后续的访问令牌刷新流程。

7.2 授权码鉴别流程

7.2.1 概述

本节介绍如何使用基于授权码的鉴别流程进行终端用户身份的鉴别。

授权码鉴别流程适用于可以安全保存依赖方密钥的依赖方，依赖方密钥用于在与授权服务器通信时，安全鉴别依赖方的身份。

在授权码鉴别流程中，本标准规定了授权服务器应具备的两个主要的功能接口：

a） 授权端点：执行终端用户的鉴别和授权；

b） 令牌端点：执行令牌的发放和验证。

在授权码鉴别流程中，授权端点给依赖方返回授权码，依赖方用授权码从令牌端点换取 ID 令牌和访问令牌。授权码交换访问令牌之前，授权服务器可以鉴别依赖方。

所有与授权端点以及令牌端点的通信应使用 GM/T 0024—2014 中定义的安全通信协议。

7.2.2 授权码流程步骤

授权码流程包括以下步骤：

a） 依赖方构造鉴别请求，该请求包含所需的所有请求参数；

b） 依赖方将请求发送到身份服务提供方的授权服务器；

c） 授权服务器鉴别终端用户；

d） 授权服务器获取终端用户许可/授权；

e） 授权服务器将终端用户重定向到依赖方，此重定向消息包含授权码；

f） 依赖方使用第 e）步中获取的授权码向授权服务器的令牌端点发起请求；

g） 依赖方收到包含 ID 令牌和访问令牌的响应；

h） 依赖方验证 ID 令牌并提取终端用户的主体标识符。

7.2.3 授权端点

7.2.3.1 鉴别请求

鉴别请求由依赖方构造，用于请求授权服务器对终端用户进行身份鉴别。

授权服务器通过授权端点执行对终端用户的身份鉴别。授权端点应支持使用 HTTP 的 GET 方法和 POST 方法。依赖方可以使用 HTTP 的 GET 或 POST 方法来将授权请求发送到授权服务器。本标准定义以下请求参数，用于构建鉴别请求：

a） 〈scope〉[必选]

请求访问的资源范围，鉴别请求的 scope 参数应包含参数值 openid。如果〈scope〉参数不包含参数值 openid，则说明该请求不是本标准定义的协议请求，本标准不对此请求操作定义。参数〈scope〉也可能包含其他参数值。应该忽略不能理解的〈scope〉参数值。范围值见 9.4.1。

b） 〈response_type〉[必选]

响应类型值，设定该参数的值为 code，表示使用授权码鉴别流程。

c) 〈client_id〉[必选]

依赖方的标识符,用于授权服务器识别依赖方的标识符。

d) 〈redirect_uri〉[必选]

依赖方用于接收身份服务提供方响应消息的 URI,身份服务提供方将响应发送到该重定向的 URI。该 URI 应完全匹配依赖方在身份服务提供方预注册的重定向 URI,匹配方式采用统一资源标识符(见 RFC 3986)中定义的匹配方式(如字符串比较)。通常,重定向 URI 应当使用 HTTPS 发送。如果要使用 HTTP 协议,依赖方类型应是具有保密能力的依赖方,并且身份服务提供方允许使用 HTTP 协议的重定向 URI。

e) 〈state〉[推荐]

依赖方用于维护请求和响应之间状态的字符串,该值对除身份服务提供方和依赖方外的其他实体均不可见。授权服务器在将用户代理重定向回到依赖方时,在其 URI 中包含该参数,以防止跨站点请求伪造攻击。

f) 〈response_mode〉[可选]

响应模式,用于通知授权端点返回参数的方法。该参数的参数值如下:

1) query:当重定向至依赖方时,通过将响应参数添加到 redirect_uri 的查询部分来返回参数,授权码鉴别流程中,默认的响应模式的值为 query;
2) fragment:当重定向至依赖方时,通过将响应参数添加到 redirect_uri 的片段部分来返回参数。一般用于隐式鉴别流程或混合鉴别流程中。当〈response_type〉值为 token 时,默认的响应模式的值为 fragment。

g) 〈nonce〉[可选]

用于将 ID 令牌与依赖方会话相关联的字符串值,能够抵御重放攻击。该值在授权过程中保持不变。该参数的信息熵应足够大,以防止攻击者猜测该值。

h) 〈display〉[可选]

ASCII 字符串值,指定授权服务器向终端用户显示界面的方式。该参数的参数值如下:

1) page:以用户代理的全页面方式呈现,如未指定显示参数,此为默认的显示模式;
2) popup:以用户代理的合适大小的弹出窗口呈现;
3) touch:以设备的触摸界面呈现;
4) wap:以手机端界面呈现。

授权服务器也可以尝试检测当前用户代理,并选择适当的显示模式。

i) 〈prompt〉[可选]

ASCII 字符串值,指定授权服务器是否提示终端用户重新进行身份鉴别和申请授权,以空格分隔且区分大小写。该参数的参数值如下:

1) none:该参数值表示授权服务器不显示用于身份鉴别和申请授权的用户界面。〈prompt〉值为 none 时,若出现以下情况,则会返回错误信息(见 7.2.3.6):终端用户尚未被鉴别,依赖方没有在注册阶段设置该参数值,或不符合其他条件。
2) login:该参数值表示授权服务器应提示终端用户重新进行身份鉴别。如果不能重新鉴别终端用户,则应返回错误信息,通常为 login_required。
3) consent:该参数值表示授权服务器给依赖方返回信息之前,应提示终端用户是否同意。如果不能获得同意,则应返回错误信息,通常为 consent_required。
4) select_account:该参数值表示授权服务器应提示终端用户选择使用一个用户账户。该参数通常用来提示拥有多个账户的终端用户,从当前会话的多个账户中选择一个。如果不能获得终端用户的其中一个账户,则应返回错误信息,通常为 account_selection_required。

依赖方使用 prompt 参数确保终端用户仍在当前会话并关注到该请求。如果此参数同时包含 none

值和其他值，则返回错误信息。

j) 〈max_age〉[可选]

最大鉴别有效期。指从上一次终端用户鉴别后的最大鉴别有效时间(秒)，如果经过的时间大于该值，则身份服务提供方应重新验证终端用户。当使用 max_age 时，ID 令牌应包括 auth_time 参数(鉴别终端用户的时间，见 8.1.2)。

k) 〈ui_locales〉[可选]

终端用户的首选语言和用户界面脚本，由语言标签值 BCP47[RFC5646]列表表示，以空格分隔，并按照需求排序。例如，值“FR-CA FR en”代表首选加拿大使用的法语，然后是法语(没有指定具体区域)，其次是英语(没有指定具体区域)。如果身份服务提供方不支持某些要求的语言环境，不应导致错误。

l) 〈id_token_hint〉[可选]

该值是依赖方在本次请求前已经获得的、关联此终端用户的 ID 令牌，此 ID 令牌可作为会话索引进行传输，索引得到当前或曾经通过鉴别的终端用户和依赖方建立的会话。如果被该值确定的终端用户已经登录或者在该次请求中登录，那么授权服务器应返回肯定的答复，否则应返回错误信息，如 login_required。当 prompt＝none 时，应该使用参数 id_token_hint，如果没有使用该参数，可能返回 invalid_request 错误。如果鉴别请求中不包含该参数，不应导致错误。

如果依赖方从身份服务提供方收到的 ID 令牌是加密的，依赖方应解密出签名的 ID 令牌，然后使用解密出来的已签名 ID 令牌作为 id_token_hint 值。依赖方可以使用授权服务器已知的密钥重新加密签名的 ID 令牌，并使用重新加密的 ID 令牌作为 id_token_hint 值。

m) 〈login_hint〉[可选]

该值为标识符或电子邮件地址等类型的字符串，用于告知授权服务器终端用户可以用该标识符登录。

n) 〈acr_values〉[可选]

请求鉴别上下文类引用值。该值是由空格分隔的字符串，指定了授权服务器用来处理授权请求时使用的 acr 值(见 8.1.2)，并按照出现的顺序进行排序。满足身份鉴别执行流程的身份鉴别上下文类通过定义的 acr 声明值(见 8.1.2)返回。该参数要求 acr 声明作为自选声明。

鉴别请求中可能还会发送其他参数，见 7.3.3、7.4.3、9.2 和 9.4 定义的授权请求参数和参数值。

另外，在实现协议时，本标准定义的协议请求和响应参数可以通过以下两种方式进行传递：

——值传递：将协议请求或响应中的参数及参数值直接附加在协议消息中进行传递；

——引用传递：将协议请求或响应中的参数及参数值通过 HTTP 机制的 URI 引用进行传递，在协议请求消息中不直接包含参数值，而是在请求消息中包含一个引用，即包含一个 URI，该 URI 指向一个资源对象，该资源对象中包含请求的参数及参数值。

具体的实现方法和要求不在本标准的规定范围内。

7.2.3.2 鉴别请求验证

授权服务器在收到请求后，应进行如下验证：

a) 授权服务器应验证鉴别请求的有效性，以确保所有必选参数都存在且有效；

b) 验证是否包含〈scope〉参数以及 scope 参数值中是否包含 openid，不包含 openid 值，则表明不是本协议规定的请求；

c) 授权服务器应遵循本标准，验证所有必选参数的有效性；

d) 如果 ID 令牌请求存在 sub 声明(见 8.1.2)，只有当 sub 值指定的终端用户和授权服务器有活跃会话，或者授权服务器已经鉴别该终端用户时，授权服务器才能够响应此请求。对其他终端用户，授权服务器则不能返回 ID 令牌或访问令牌。这种类型的请求也可以使用 id_token_

hint 参数或通过请求特定的声明值(实现应支持 claims 参数)(见 9.4.2)来实现。

当授权服务器发现无法识别的请求参数时,应忽略该请求参数。

当授权服务器发生错误时,应返回错误响应(见 7.2.3.6)。

7.2.3.3 授权服务器鉴别终端用户

如果请求有效,身份服务提供方根据请求参数值判定终端用户是否通过鉴别。身份服务提供方对终端用户进行身份鉴别的方法(如用户名和口令)本标准不作规定。身份服务提供方身份鉴别的用户界面可由身份服务提供方呈现,呈现的方法由身份服务提供方根据所用的请求参数值和鉴别方法决定。

在下列情况下授权服务器应重新鉴别终端用户:

a) 终端用户尚未经过身份鉴别;

b) 该鉴别请求中包含的 prompt 参数值为 login。在这种情况下,授权服务器应重新鉴别终端用户,即使终端用户已经通过身份鉴别。

在下列情况下,授权服务器不能与终端用户进行交互:该鉴别请求中包含的 prompt 参数值为 none。此种情况下,如果终端用户尚未经过身份鉴别或无法进行鉴别,授权服务器应返回一个错误信息。

当授权服务器与终端用户交互时,授权服务器应采用适当措施阻止跨站请求伪造和点击劫持攻击。

7.2.3.4 授权服务器获取终端用户许可/授权

终端用户成功通过身份鉴别后,在给依赖方发放信息之前,身份服务提供方应从终端用户获取授权决定。在所使用的请求参数满足要求的情况下,授权决定可以通过推送与终端用户交互的对话框实现,使得终端用户清楚被授权的内容,以便执行授权命令;或者根据终端用户提前设置的授权规则来作授权决定;或者通过其他的方式实现。信息发放机制不在本标准的规定范围内,身份服务提供方可以使用恰当的方式发放许可/授权信息。

7.2.3.5 鉴别成功响应

终端用户成功通过身份鉴别后,身份服务提供方的授权端点应使用本条定义的“鉴别成功响应”消息来响应依赖方发送的鉴别请求消息。

当使用授权码鉴别流程时,授权服务器应发送授权码给依赖方,通常通过重定向的方式实现。授权服务器向重定向端点 URI 的查询组件添加如下参数(先使用 UTF-8 对参数进行编码后,再使用“application/x-www-form-urlencoded”[RFC1867]格式编码):

a) 〈code〉[必选]

由授权服务器产生的授权码。为降低泄露的风险,该授权码应在发放后短时间内失效。推荐授权码最长生命周期为 10 min。依赖方不得重复使用该授权码。授权服务器应将授权码与依赖方的标识符、重定向 URI 进行绑定。在后续的授权码换取访问令牌的过程中,如果授权码被重复使用,授权服务器应拒绝请求,并撤销此前基于该授权码所发放的所有访问令牌。

b) 〈state〉

如果依赖方的鉴别请求中含有此参数,则鉴别响应中也应包含此参数。该参数的值与依赖方发送的鉴别请求中的〈state〉值相同。

依赖方应忽略未识别的响应参数。本标准对授权码的字符串长度不作定义。依赖方不宜对字符串长度做出假定。身份服务提供方应在其服务文档中说明其发放的所有参数值的长度。

授权码的发放应采用 GM/T 0024—2014 中定义的安全通信协议进行传输。

7.2.3.6 鉴别错误响应

当终端用户的鉴别失败、终端用户拒绝授权或出现其他错误时,身份服务提供方的授权端点应使用

本条定义的“鉴别错误响应”消息来响应由依赖方发送的鉴别请求消息。

身份服务提供方，应在鉴别错误响应中包含以下错误响应参数。除非依赖方的重定向 URI 是无效的，否则授权服务器应将鉴别请求中指定的状态参数和错误响应参数返回到依赖方重定向 URI 的查询部分，此外不应返回其他参数。

本标准定义了如下错误响应参数：

a) interaction_required：表示授权服务器应与终端用户交互。当鉴别请求的 prompt 参数值为 none（见 7.2.3.1），且在不给终端用户显示用户交互界面的情况下不能完成鉴别请求，应返回该错误代码。

b) login_required：表示授权服务器应对终端用户进行身份鉴别。当鉴别请求的 prompt 参数值为 none，且在不显示用户身份鉴别界面的情况下不能完成鉴别请求，应返回该错误。

c) account_selection_required：表示终端用户应选择一个授权服务器会话。当鉴别请求的 prompt 参数值为 none，且在不给终端用户显示用户界面以提示使用一个授权服务器会话的情况下，应返回该错误代码。

d) consent_required：表示授权服务器应获取终端用户的授权许可。当鉴别请求的 prompt 参数值为 none，且在不给终端用户显示用户同意界面的情况下，应返回该错误代码。

如果鉴别请求通过引用传递的方式（见 7.2.3.1）进行传递时，当出现以下情况：引用指向的资源内容中不包含请求对象，或请求对象中包含无效数据，或者依赖方所使用的代表引用传递方式的参数并不适用于身份服务提供方，应返回错误代码，本标准对此类错误代码不作规定。

本标准定义了如下错误响应参数：

1) 〈error〉[必选]

错误代码；

2) 〈error_description〉[可选的]

可读的关于该错误的文字说明，使用 ASCII 编码；

3) 〈error_uri〉[可选的]

包含有关该错误的附加信息；

4) 〈state〉

如果鉴别请求中包含〈state〉参数，则鉴别错误响应中应包含该参数。参数值等于依赖方发送的鉴别请求中的〈state〉参数值。

7.2.3.7 鉴别响应验证

依赖方应验证收到的鉴别响应中的所有必选参数是否有效，应忽略不能识别的响应参数。应验证〈state〉参数值是否与其在鉴别请求中的〈state〉参数值是否相同。

7.2.4 令牌端点

7.2.4.1 令牌请求

依赖方向令牌端点发出包含授权码的令牌请求，以获取访问令牌。依赖方应在请求的主体部分添加如下参数（参数经过 UTF-8 编码后，再使用“application/x-www-form-urlencoded”格式编码）：

a) 〈grant_type〉[必选]

参数值应为 “authorization_code”；

b) 〈code〉[必选]

从授权服务器获得的授权码；

c) 〈redirect_uri〉

如果依赖方在7.2.3的鉴别请求中包含此参数，则在该请求中也应包含此参数。应确保该参数两次的值相同；

d) 〈client_id〉

如果依赖方未按照6.2.4的要求进行身份鉴别时，则依赖方应在该请求中添加此参数。

授权服务器应：

——要求对有保密能力型的依赖方或任何被发放过依赖方身份凭据(或被其他鉴别要求所约束)的依赖方进行身份鉴别；

——如果需要鉴别该依赖方，则执行鉴别流程；

——确保发放授权码给正确的依赖方，即通过了身份鉴别的有保密能力型依赖方，或是请求中〈client_id〉参数所标识的无保密能力型依赖方；

——验证授权码是否有效。

7.2.4.2 令牌请求验证

身份服务提供方的令牌端点应验证令牌请求，验证方式如下：

a) 如果身份服务提供方发放了依赖方身份凭据或者提供了其他鉴别依赖方的方式，则应鉴别依赖方；

b) 确保授权码颁发给能够通过身份鉴别的依赖方；

c) 验证授权码的有效性；

d) 验证授权码未被重复使用；

e) 确保redirect_uri参数值和包含在初始鉴别请求中的redirect_uri参数值是相同的。如果依赖方只有一个已注册的redirect_uri值，且redirect_uri参数值在该请求中不存在，则身份服务提供方可选择返回错误(因为依赖方在令牌请求中应包括该参数)，也可选择继续操作(如在此种情况下省略该参数)；

f) 验证该授权码由本标准定义的鉴别成功响应返回。

7.2.4.3 令牌成功响应

当验证来自依赖方的令牌请求是有效的请求之后，身份服务提供方的令牌端点返回成功的响应，其中包含ID令牌和访问令牌。该响应使用application/ json(见RFC 4627)中定义的类型。

本标准规定的响应参数如下：

a) 〈id_token〉[必选]

与鉴别会话关联的ID令牌(见8.1.2)。

所有包含令牌、凭据或者其他敏感信息的令牌响应中应包括表1中HTTP响应头字段和头字段的值。

表1 HTTP响应的头字段及其值

头字段	头字段的值
Cache-Control	no-store
Pragma	no-cache

依赖方应忽略无法识别的响应参数。

b) 〈access_token〉[必选]

授权服务器发放的访问令牌。

c) 〈token_type〉[必选]

身份服务提供方与依赖方已经协商好的令牌类型，令牌类型的定义和使用不在本标准的规定范围内。

d) 〈expires_in〉[推荐]

访问令牌的生命周期，以秒为单位。例如，“3600”表示该访问令牌将在响应发出1小时后失效。如果本参数被省略，授权服务器应通过其他方式提供失效时间，或公布缺省值。

e) 〈scope〉

如果该参数的值与依赖方鉴别请求中的〈scope〉参数值相同，则该参数是可选的；其他情况下，该参数是必选的。

f) 〈state〉

如果依赖方的鉴别请求中含有此参数，则该响应中也应包含此参数。该参数的值与依赖方鉴别请求中的〈state〉值相同。

依赖方应忽略未识别的响应参数。身份服务提供方应在其服务文档中说明其发放的所有参数值的长度。

7.2.4.4 令牌错误响应

如果令牌请求是无效的或未经授权的，授权服务器应返回错误响应。HTTP响应主体采用application/json(见RFC 4627)中定义的类型。授权服务器返回状态码为400(Bad Request)的HTTP响应，并在响应中包含如下参数：

a) 〈error〉[必选]

ASCII格式的错误代码，有以下类型：

1) invalid_request 表示该请求缺失了必选参数，或包含了不被支持的参数值(但如果是授权许可是不被支持的类型，返回错误码应为invalid_grant)，或重复包含了某一参数，或包含了多个凭据，或使用了多种依赖方身份鉴别的方式等。
2) invalid_client 表示鉴别依赖方的身份失败。授权服务器可返回状态码为401的HTTP响应，用以表明支持哪些HTTP鉴别方案。
3) invalid_grant 表示依赖方提供的授权许可(例如，授权码，资源拥有者口令凭据)或刷新令牌是无效的，或过期的，或被撤销的，或与授权请求中提供的重定向端点URI不匹配，或发放给另外的依赖方。
4) unauthorized_client 表示授权服务器不允许该依赖方使用当前授权许可类型。
5) unsupported_grant_type 授权服务器不支持当前使用的授权许可类型。
6) invalid_scope 所请求的访问受保护资源范围无效、未知、格式有误或是超出了终端用户授权的范围。

〈error〉参数的值不应包含%x20-21/%x23-5B/%x5D-7E集合之外的字符。

b) 〈error_description〉[可选]

终端用户可读的关于错误的附加说明，使用ASCII编码。

c) 〈error_uri〉[可选]

用于标识包含有终端用户可读的、关于该错误更多信息的网页URI。该参数的值应遵循URI-reference语法，并且不应包含%x20-21/%x23-5B/%x5D-7E集合之外的字符。

7.2.4.5 令牌响应验证

依赖方验证令牌响应，验证规则如下：

a) 依赖方应验证所有的必选参数是否正确、有效，应验证参数值是否和令牌请求中请求的数据一致；

b) 遵循 ID 令牌的验证规则(见 7.2.4.7);
c) 遵循访问令牌的验证规则(见 7.2.4.8)。

7.2.4.6 ID 令牌

ID 令牌的内容见 8.1.2。当使用授权码鉴别流程时,ID 令牌的声明需要包括如下扩展要求:

〈at_hash〉[可选]

访问令牌的杂凑值。将访问令牌值的 ASCII 码八位位组表示的编码进行杂凑运算,然后使用 Base64url 对杂凑值的最左边一半进行编码,并作为该参数值,杂凑算法使用 JSON 令牌的 alg 参数指明的杂凑算法(见 8.2)。例如,如果〈alg〉值是 SM3,用 SM3 算法(见 GB/T 32905—2016)计算访问令牌杂凑值,然后采取最左边的 128 位并用 Base64url 编码。该〈at_hash〉值是字符串,区分大小写。

7.2.4.7 ID 令牌验证

依赖方应用下列方式验证令牌响应中的 ID 令牌:

a) 如果 ID 令牌是加密的,使用该依赖方注册过程中设置的密钥和算法,对 ID 令牌进行解密。依赖方与身份服务提供方的密钥协商,可以在依赖方注册过程中实现,具体实现过程不在本标准的规定范围内。如果依赖方与身份服务提供方协商使用加密的 ID 令牌,但 ID 令牌没有加密,则依赖方应拒绝该令牌。
b) 身份服务提供方的发布方标识符(见 6.1.3)应与〈iss〉参数完全匹配。
c) 依赖方应验证 ID 令牌 aud 声明中的 client_id 值,该 client_id 值在 iss 声明所指定的发放方注册。aud 声明可能包含一个数组,该数组包含多个依赖方标识符。如果 ID 令牌没有把依赖方列为有效的接收方,或者它包含不受依赖方信任的接收方,该 ID 令牌应被拒绝。
d) 如果 ID 令牌包含多个接收者,依赖方应该验证该令牌中是否包含 azp 声明(见 8.1.2)。
e) 如果 azp 声明存在,依赖方应该验证 client_id 是 azp 声明中的接收者列表中的某个元素。
f) 如果通过依赖方和令牌端点之间直接通信来传送 ID 令牌,可以用 TLS 服务器验证身份服务提供方的身份,从而代替令牌签名的验证。依赖方应根据与身份服务提供方协商的签名验证方式验证 ID 令牌的签名。依赖方应使用身份服务提供方提供的密钥。依赖方与身份服务提供方的具体签名加密协商过程不在本标准的规定范围内。
g) alg 参数值应为默认的国家密码算法或依赖方在注册过程中定义的 id_token_signed_response_alg 参数所指定的算法。
h) 如果 JSON 令牌的参数 alg 指定使用基于 MAC 的算法,如 HMAC SM3,使用依赖方的 client_secret 值的 UTF-8 编码作为密钥,以验证签名。
i) 当前时间应早于 exp 参数见 8.1.2 所代表的时间。
j) iat 声明见 8.1.2 可以被用来拒绝过于陈旧的令牌,也可以限制 nonce 的存储时间以防止被攻击。该声明可接受的范围值由依赖方指定。
k) 如果请求中包含 nonce 参数值,那么 nonce 参数在 ID 令牌中应存在,并且要对该值进行检查,以确认其与请求中的 nonce 参数值相同。依赖方应检查该值以防止重放攻击。用于检测重放攻击的方法由依赖方指定。
l) 如果请求 acr 声明,依赖方应检查声明的值是否合适。本标准不对 acr 声明值的含义和处理进行规定。
m) 依赖方检查 auth_time 参数值,如果该参数值表示此终端用户的最后一次鉴别在很久之前,依赖方应要求重新对该终端用户进行身份鉴别。

7.2.4.8 访问令牌验证

当使用授权码鉴别流程时，ID 令牌和访问令牌是从令牌端点返回的。如果 ID 令牌包含 at_hash 声明（见 7.2.4.6），依赖方可以使用和隐式鉴别流程相同的方式来验证访问令牌。

7.3 隐式鉴别流程

7.3.1 概述

本条介绍如何使用隐式鉴别流程进行终端用户身份的鉴别。

隐式鉴别流程主要用于在浏览器中使用脚本语言实现的依赖方或本机应用程序类型的依赖方。由于这类依赖方不具备安全保存机密信息的能力，因此该流程中的授权服务器不执行依赖方的身份鉴别。

当使用隐式鉴别流程时，所有的令牌从授权端点返回，不使用令牌端点。授权端点进行终端用户的鉴别，该过程通过将用户代理（如浏览器）重定向到授权服务器的授权端点进行鉴别和授权。

终端用户与授权端点的通信应使用 GM/T 0024—2014 中的安全通信协议。

7.3.2 隐式鉴别流程步骤

隐式鉴别流程的步骤如下：

a) 依赖方构建包含所需请求参数的鉴别请求；
b) 依赖方将请求发送到授权服务器；
c) 授权服务器鉴别终端用户；
d) 授权服务器获取终端用户许可/授权；
e) 授权服务器将终端用户重定向到依赖方，并返回 ID 令牌，如果请求访问令牌，则同时返回访问令牌；
f) 依赖方验证 ID 令牌并获取终端用户的主体标识符。

7.3.3 授权端点

7.3.3.1 鉴别请求

当使用隐式鉴别流程时，除本节规定的差异外，该过程其他部分与授权码鉴别流程相同，同 7.2.3.1 中的定义。

a) 〈response_type〉[必选]

用于确定使用的鉴别流程类型。当使用隐式鉴别流程时，该参数值为 id_token token 或者 id_token。当值为 id_token 时不返回访问令牌，当值为 id_token token 时同时返回 ID 令牌和访问令牌。

b) 〈redirect_uri〉[必选]

依赖方用于接收身份服务提供方响应消息的 URI 地址，身份服务提供方将响应发送到该重定向的 URI 地址。该 URI 应完全匹配依赖方在身份服务提供方注册的重定向 URI 值，匹配方式采用统一资源标识符（见 RFC 3986）中定义的匹配方式（如字符串比较）。当使用隐式鉴别流程时，重定向的 URI 不能使用 HTTP 协议，除非依赖方是本机应用程序，在这种情况下，可能会使用 localhost 作为 http: scheme 的主机名。

7.3.3.2 鉴别请求验证

当使用隐式鉴别流程时，该过程与授权码鉴别流程相同，同 7.2.3.2 中的定义。

7.3.3.3 授权服务器鉴别终端用户

当使用隐式鉴别流程时，鉴别终端用户的过程与授权码鉴别流程相同，同 7.2.3.3 中的定义。

7.3.3.4 授权服务器获取终端用户许可/授权

当使用隐式鉴别流程时，该过程与授权码鉴别流程相同，同 7.2.3.4 中的定义。

7.3.3.5 鉴别成功响应

当使用隐式鉴别流程时，所有的响应参数添加到重定向 URI 的片段部分，除非指定了不同的响应模式。

本标准定义的以下参数将从授权端点返回：

a) 〈id_token〉[必选]

如 7.2.4.3 所述。

b) 〈access_token〉[可选]

表示返回访问令牌，当 response_type 的值为 id_token 时该参数不返回。

c) 〈token_type〉[可选]

身份服务提供方与依赖方已经协商好的访问令牌类型，令牌类型的定义和使用不在本标准的规定范围内，当 response_type 的值为 id_token 时该参数不返回。

d) 〈expires_in〉[推荐]

如 7.2.4.3〈expires_in〉参数所述。

e) 〈scope〉

如 7.2.4.3〈scope〉参数所述。

f) 〈state〉

如 7.2.4.3〈state〉参数所述。

7.3.3.6 鉴别错误响应

当使用隐式鉴别流程时，除本条规定的差异外，该过程其他部分与授权码鉴别流程相同，同 7.2.3.6 中的定义。

当使用隐式鉴别流程时，所有的错误响应参数添加到重定向 URI 的片段部分，除非指定了不同的响应模式。

7.3.3.7 重定向的 URI 片段处理

由于响应参数在重定向的 URI 片段中返回，用户代理应先解析片段的编码值，再将其传递给依赖方。有关 URI 片段的处理实现，本标准不作规定。

7.3.3.8 鉴别响应验证

当使用隐式鉴别流程时，依赖方应按照如下规定验证响应：

a) 依赖方应验证收到的鉴别响应中的所有必选参数是否正确、有效，应忽略不能识别的响应参数。应验证〈state〉参数值是否与其在鉴别请求中的〈state〉参数值相同。

b) 遵循 ID 令牌的验证规则(见 7.3.3.11)。

c) 遵循访问令牌的验证规则(见 7.3.3.9)，除非使用的〈response_type〉的值为 id_token。

7.3.3.9 访问令牌验证

在使用隐式鉴别流程中，当 response_type 为 id_token token 时，ID 令牌和访问令牌同时从授权端

点返回的。依赖方对访问令牌的验证应做到以下几点：

a) 将访问令牌按照 ID 令牌的〈alg〉参数中指定的杂凑算法进行杂凑运算。例如，如果〈alg〉是 SM3_SM2，所使用的杂凑算法是 SM3(见 GB/T 32905—2016)。

b) 取杂凑值最左边的一半，使用 Base64url 对其进行编码。

c) ID 令牌的 at_hash 参数值应与先前步骤中所产生的值匹配。

7.3.3.10 ID 令牌

ID 令牌的内容见 8.1.2。当使用隐式鉴别流程时，ID 令牌声明需要提供以下额外参数：

a) 〈nonce〉

隐式鉴别流程中必选。

b) 〈at_hash〉

访问令牌的杂凑值。将访问令牌值的 ASCII 码八位位组表示的编码进行杂凑运算，然后使用 Base64url 对杂凑值的最左边一半进行编码，并作为该参数值，杂凑算法使用 JSON 令牌的 alg 参数指明的杂凑算法(见 8.2)。例如，如果〈alg〉值是 SM3，用 SM3 算法(见 GB/T 32905—2016)计算访问令牌杂凑值，然后采取最左边的 128 位并用 Base64url 编码。该〈at_hash〉值是字符串，区分大小写。

如果从端点授权发放 ID 令牌的同时发放了 access_token 值，即 response_type 的值为 id_token token 的情况下，该参数是必选的。如果 response_type 的值为 id_token，即没有访问令牌发放，该参数可能不会被使用。

7.3.3.11 ID 令牌验证

当使用隐式鉴别流程时，除本条规定的差异外，ID 令牌验证与授权码鉴别流程中 ID 令牌的验证相同(见 7.2.4.7)。本条规定的 ID 令牌的验证包括以下两点：

a) 依赖方验证 ID 令牌的签名时，应根据依赖方与身份服务提供方协商好的签名验证方式进行验证；

注：依赖方与身份服务提供方协商签名验证的方式不在本标准的规定范围内，依赖方在身份服务提供方注册时，可以与身份服务进行协商。

b) 应对 nonce 参数值进行检查，确认其和鉴别请求中的 nonce 值相同。依赖方使用该参数防止重放攻击。

7.4 混合鉴别流程

7.4.1 概述

本条介绍如何使用混合鉴别流程进行终端用户的身份鉴别。当使用混合鉴别流程时，有的令牌是从授权端点返回，有的令牌则从令牌端点返回。

对于没有能力安全保存机密信息的依赖方，不能使用授权码换取刷新令牌，因此授权码鉴别流程和隐式鉴别流程之外还需要混合鉴别流程。混合鉴别流程是授权码鉴别流程与隐式鉴别流程的结合，该流程允许依赖方请求 ID 令牌、访问令牌和授权码的任意组合。例如，在以下情况可使用混合鉴别流程：依赖方需要立即使用 ID 令牌去访问终端用户的身份信息，并且还需要利用授权码请求刷新令牌以获得长期访问资源的权限。

当使用混合鉴别流程时，除 7.4 指明的差异外，对授权端点和令牌端点的使用要求与授权码鉴别流程中授权端点和令牌端点的使用要求相同(见 7.2.3 和 7.2.4)。

7.4.2 混合鉴别流程步骤

混合鉴别流程的步骤如下：

a) 依赖方准备包含所需的请求参数的鉴别请求；
b) 依赖方将请求发送到授权服务器；
c) 授权服务器鉴别终端用户；
d) 授权服务器获取终端用户许可/授权；
e) 授权服务器将终端用户返回到依赖方并携带授权码，并根据响应类型，返回一个或多个附加参数；
f) 依赖方使用第 e)步收到的授权码向令牌端点发出请求；
g) 依赖方收到包含 ID 令牌和访问令牌的响应；
h) 依赖方验证 ID 令牌并获取终端用户的主体标识符。

7.4.3 授权端点

7.4.3.1 鉴别请求

当使用混合鉴别流程时，除本条规定的差异外，该过程其他部分与授权码鉴别流程定义的鉴别请求相同。

本条规定了以下请求参数的使用方法：

〈response_type〉[必选]

当使用混合鉴别流程时，该值为 code id_token、code token 或 code id_token token。

7.4.3.2 鉴别请求验证

当使用混合鉴别流程时，该过程与授权码鉴别流程相同，同 7.2.3.2 中的定义。

7.4.3.3 授权服务器鉴别终端用户

当使用混合鉴别流程时，该过程与授权码鉴别流程相同，同 7.2.3.3 中的定义。

7.4.3.4 授权服务器获取终端用户许可/授权

当使用混合鉴别流程时，该过程与授权码鉴别流程相同，同 7.2.3.4 中的定义。

7.4.3.5 鉴别成功响应

当使用混合鉴别流程时，除本节规定的差异外，该过程其他部分与隐式鉴别流程相同，同 7.3.3.5 中定义。

授权端点返回以下参数：

a) 〈id_token〉

ID 令牌，〈response_type〉的值为 code id_token 或者 code id_token token 时返回该参数。

b) 〈access_token〉

访问令牌，当〈response_type〉的值为 code token 或者 code id_token token 时返回该参数(token_type 参数值与此参数使用相同)。

c) 〈code〉

授权码，使用混合鉴别流程时应返回该参数。

7.4.3.6 鉴别错误响应

当使用混合鉴别流程时，除本节规定的差异外，该过程其他部分与隐式鉴别流程相同，同 7.3.3.6 中的定义。

如果终端用户拒绝请求或终端用户鉴别失败，在没有指定其他响应模式的情况下，所有的错误响应参数应添加到重定向 URI 的片段部分。

7.4.3.7 重定向的 URI 片段处理

当使用混合鉴别流程时，由于响应参数在重定向的 URI 片段中返回，依赖方需要使用用户代理解析片段编码值，并将其传递给依赖方的处理逻辑。有关 URI 片段的处理实现，本标准不做规定。

7.4.3.8 鉴别响应验证

当使用混合鉴别流程时，依赖方应按如下方式验证鉴别响应：

a) 依赖方应验证收到的鉴别响应中的所有必选参数是否正确、有效，应忽略不能识别的响应参数。应验证〈state〉参数值是否与其在鉴别请求中的〈state〉参数值相同；

b) 当 response_type 值为 code id_token 或 code id_token token 时，按照 ID 令牌验证规则（见 7.4.3.11）验证；

c) 当 response_type 的值为 code token 或 code id_token token 时，按照访问令牌的验证规则（见 7.4.3.9）验证；

d) 按照授权码验证规则（见 7.4.3.10）验证授权码。

7.4.3.9 访问令牌验证

当使用混合鉴别流程时，使用隐式鉴别流程中的访问令牌验证方式（见 7.3.3.9）验证。

7.4.3.10 授权码验证

为了验证从授权端点与 ID 令牌同时发出的授权码，依赖方应做到以下几点：

a) 将授权码按照 ID 令牌的 alg 参数指定的杂凑算法进行杂凑运算。例如，如果〈alg〉是 SM3_SM2，所使用的杂凑算法是 SM3（见 GB/T 32905—2016）；

b) 取杂凑值最左边的一半，使用 Base64url 对其进行编码；

c) 如果 ID 令牌中存在 c_hash 参数（见 7.4.3.11），该参数的值应与先前步骤中所产生的值匹配。

7.4.3.11 ID 令牌

ID 令牌的内容见 8.1.2。当使用混合鉴别流程时，ID 令牌声明需要有以下扩展的要求：

a) 〈nonce〉

混合鉴别流程中该参数为必选。

b) 〈at_hash〉

访问令牌的杂凑值。将访问令牌的 ASCII 码八位位组表示的编码进行杂凑，然后对杂凑值的最左边一半使用 Base64url 编码后的值作为该参数的值，杂凑算法使用 ID 令牌的 alg 参数对应的杂凑算法。例如，如果〈alg〉值是 SM3_SM2，用 SM3 算法（见 GB/T 32905—2016）计算访问令牌杂凑值，然后使用最左边的 128 位进行 Base64url 编码。该〈at_hash〉值是字符串，区分大小写。

如果从授权端点发放 ID 令牌的同时发放访问令牌，即〈response_type〉的值为 codeid_token token 的情况下，该参数为必选。如果〈response_type〉的值为其他，则该参数为可选。

c) 〈c_hash〉

授权码的杂凑值。该值由授权码值的 ASCII 码八位位组表示的编码进行杂凑，然后对杂凑值的最左边一半使用 Base64url 编码后的值，杂凑算法使用 JSON 令牌的 alg 参数对应的杂凑算法（见 8.2）。例如，如果 alg 是 SM3_SM2，用 SM3 算法（见 GB/T 32905—2016）计算授权码杂凑值，然后采取最左边的 128 位并用 Base64url 编码。该 c_hash 值是字符串，区分大小写。

如果从端点授权发放 ID 令牌的同时发放授权码，即〈response_type〉的值为 codeid_token 或者 codeid_token token 的情况下，则该参数为必选。如果〈response_type〉的值为其他，则该参数为可选。

7.4.3.12 ID 令牌验证

当使用混合鉴别流程时，应以 7.3.3.11 所述同样的方式验证 ID 令牌。

7.4.4 令牌端点

7.4.4.1 令牌请求

当使用混合鉴别流程时，令牌请求与授权码鉴别流程相同，同 7.2.4.1 中的定义。

7.4.4.2 令牌请求验证

当使用混合鉴别流程时，令牌请求验证与授权码鉴别流程相同，同 7.2.4.2 中的定义。

7.4.4.3 令牌成功响应

当使用混合鉴别流程时，令牌成功响应与授权码鉴别流程相同，同 7.2.4.3 中的定义。

7.4.4.4 令牌错误响应

当使用混合鉴别流程时，令牌错误响应与授权码鉴别流程相同，同 7.2.4.4 中的定义。

7.4.4.5 令牌响应验证

当使用混合鉴别流程时，令牌响应验证与授权码鉴别流程相同，同 7.2.4.5 中的定义。

7.4.4.6 ID 令牌

当使用混合鉴别流程时，除本节规定的差异外，从令牌端点返回的 ID 令牌与从授权端点返回的 ID 令牌（见 7.4.3.11）相同。

如果授权端点和令牌端点同时返回 ID 令牌，即〈response_type〉的参数值为 codeid_token 或者 codeid_token token 的情况下，这两个 ID 令牌的 iss 声明参数和 sub 声明（见 8.1.2）参数应是相同的。关于鉴别事件的所有声明参数应存在于这两个 ID 令牌中。如果任一 ID 令牌包含有关终端用户的声明，那么这两个 ID 令牌应该有相同的参数值。由于隐私的原因，从身份服务提供方授权端点可能返回的终端用户信息不完全包含令牌端点返回的终端用户信息。令牌端点返回的 ID 令牌〈at_hash〉声明参数值和〈c_hash〉声明参数值可以省略，因为从令牌端点返回的 ID 令牌和访问令牌已经由令牌端点采用 GM/T 0024—2014 中定义的安全通信协议进行加密。

7.4.4.7 ID 令牌验证

当使用混合鉴别流程时，从令牌端点返回的 ID 令牌应以 7.2.4.7 中定义的方式进行验证。

7.4.4.8 访问令牌

如果访问令牌同时从授权端点和令牌端点返回，即〈response_type〉的参数值为 codetoken 或者 codeid_token token 的情况下，它们的值可以是相同的也可以是不同的。需要注意的是不同的访问令牌可能由于两个端点的安全特性不同，从而使得访问令牌的生命周期和授权资源不同。

7.4.4.9 访问令牌验证

当使用混合鉴别流程时，应遵循 7.2.4.8 中定义的方式对令牌端点返回的访问令牌进行验证。

7.5 访问令牌刷新机制

7.5.1 概述

当发送到令牌端点的请求中〈grant_type〉参数值为 refresh_token 时，表示使用刷新令牌。本条定义授权服务器使用刷新令牌时的流程。

7.5.2 刷新请求

要使用刷新令牌，依赖方应根据请求中提供的 client_id 向令牌端点执行鉴别(见 6.2.4)。

授权服务器应验证刷新令牌，验证该令牌是否应发给该依赖方，并且当依赖方存在身份鉴别方法时，应验证依赖方是否通过了身份鉴别。

7.5.3 刷新成功响应

刷新令牌验证成功后，根据 7.2.4.3 规定的令牌响应进行响应，但不同的是它可能不包含 id_token。

如果 ID 令牌作为令牌刷新请求的结果，应满足以下要求：

a) 其 iss 声明值应与正常鉴别流程发放的 ID 令牌相同；
b) 其 sub 声明值应与正常鉴别流程发放的 ID 令牌相同；
c) 其 iat 声明值应代表新的 ID 令牌发出的时间；
d) 其 aud 声明值应与正常鉴别流程发放的 ID 令牌相同；
e) 如果 ID 令牌包含 auth_time 声明，其值应是正常鉴别流程身份鉴别的时间，而不是发出新的 ID 令牌的身份鉴别时间；
f) azp 声明的值必需与原始鉴别发生时发放的 ID 令牌中对应的值相同。如果原始鉴别时发放的 ID 令牌中没有 azp 声明，那么 azp 一定不能出现在新的 ID 令牌中；
g) 另外，用刷新令牌获取 ID 令牌的规则需要满足原始鉴别发生时发出 ID 令牌的规则。

7.5.4 刷新错误响应

如果刷新请求是无效的或未经授权的，则授权服务器应返回在 7.2.4.4 中定义的令牌错误响应。

7.5.5 请求和响应的安全保护要求

针对鉴别请求、令牌请求、刷新请求以及用户信息请求(见 9.3.2)，依赖方应采取合适的措施，对请求进行保护。

依赖方在发送请求时，应对请求进行加密处理，以确保请求的机密性，防止请求泄露。可选择的方法如下：

a) 采用 GM/T 0024—2014 中的安全通信协议进行加密传输；
b) 采用合适的密钥和 SM4 加密算法(见 GB/T 32907—2016)对请求中涉及敏感信息的主体部分进行加密。

为了防止依赖方否认其发出过的请求，授权服务器应要求依赖方对请求进行数字签名。服务器应该验证数字签名，以确保该请求是由合法的依赖方发出，并且确保该请求的完整性。

授权服务器的响应可能包含鉴别数据和声明，鉴别数据和声明中包括有关依赖方的敏感信息。响应内容的泄露可导致依赖方易受其他类型的攻击。本标准要求应从以下两个方面防止服务器响应的泄露：

a) 使用授权码响应类型。该响应通过 GM/T 0024—2014 保护的通道发送，在这种方式中依赖方使用 client_id 和 client_secret 进行鉴别。

b) 对于其他类型的响应，该响应需要先签名再加密。签名后的响应可以用依赖方的公钥或共享密钥加密，以作为用适当的密钥和加密算法加密的 JSON 令牌发送。

为了防止授权服务器授权否认其发出的响应，授权服务器应使用对响应进行数字签名。依赖方应验证该数字签名，以确保它是由合法的授权服务器发放，并且确保响应的完整性。

8 令牌

8.1 令牌类型

8.1.1 概述

本标准定义的协议主要涉及三类令牌：ID 令牌、访问令牌和刷新令牌。其中，ID 令牌是在终端用户成功通过身份鉴别之后，由身份服务提供方发放给依赖方的，该令牌包含了终端用户鉴别结果的声明，通常包含简单的用户标识，如用户的主体标识符；访问令牌也是身份服务提供方发放给依赖方的一种凭据，用于依赖方获取终端用户的身份信息；刷新令牌是身份服务提供方发放给依赖方的，用于重新获取访问令牌的凭据。以上令牌可使用 JSON 令牌的格式来表述，并结合密码技术来确保安全。

8.1.2 ID 令牌

ID 令牌是包含终端用户的授权声明的 JSON 令牌，其正文部分是包含终端用户声明的 JSON 对象，关于声明的具体内容见第 9 章。

下面是 ID 令牌中所使用的声明：

a) 〈iss〉[必选]

发布方标识符。

b) 〈sub〉[必选]

主体标识符。终端用户在发布方使用的唯一且不会重新分配的标识符，依赖方使用该标识符，例如 24400320 或 AItOawmwtWwcT0k51BayewNvutrJUqsvl6qs7A4。它应不超过 255 个 ASCII 字符。sub 值是字符串，区分大小写。

c) 〈aud〉[必选]

ID 令牌的接收方。对应的依赖方的标示符 client_id 应被列为其中的一个接收方。它可能还包含其他接收方的标识符。在一般情况下，该声明是区分大小写的字符串数组。在有且仅有一个接收方的特殊情况下，该值可以是单个字符串，区分大小写。

d) 〈exp〉[必选]

ID 令牌的有效时间。ID 令牌应在有效时间内使用。实现时，通常会提供不多于几分钟的时间差，以应对时钟偏移。声明值是一个 JSON 数字，代表自 1970 年 1 月 1 日 0 时 0 分 0 秒(1970-01-01T0:0:0Z)UTC 至到期时间的秒数。在 RFC 3339 中描述了时间和 UTC。

e) 〈iat〉[必选]

ID 令牌的发放时间。声明值是一个 JSON 数字，代表自 1970 年 1 月 1 日 0 时 0 分 0 秒(1970-01-01T0:0:0Z)UTC 至发放时间的秒数。

f) 〈auth_time〉

鉴别终端用户的时间。声明值是一个 JSON 数字，代表自 1970 年 1 月 1 日 0 时 0 分 0 秒(1970-01-01T0:0:0Z)UTC 至鉴别时间的秒数。当鉴别请求中包含〈max_age〉时，ID 令牌中应包含该声明。

g) 〈nonce〉

该参数用于将 ID 令牌和依赖方进行关联，以避免遭受重放攻击。参数值是字符串，区分大小写。

h) 〈acr〉[可选]

鉴别上下文类引用。该参数是 URI 字符串，指定了鉴别上下文类，表示鉴别采用合适的执行过程。当该参数值为“0”时，表示终端用户的鉴别不符合 ISO/IEC 29115:2013 中规定的 1 级要求。使用生命周期较长的浏览器 cookie 方式是安全级别为“级别 0”的鉴别方法。关于该参数值，依赖方和身份服务提供方应进行协商达成一致。〈acr〉值区分大小写。

i) 〈amr〉[可选]

鉴别方法引用。该值是 JSON 字符串数组，该数组的元素用于表示所使用的身份鉴别方法。对〈amr〉声明值的定义不在本标准的规定范围。关于该参数值，依赖方和身份服务提供方应进行协商达成一致。〈amr〉值区分大小写。

j) 〈azp〉[可选]

被授权方，即被授权的、接收该 ID 令牌的依赖方。如果 ID 令牌包含该参数，则该参数应包含该依赖方 ID。当 ID 令牌只有一个接收者并且该接收者与被授权方不同时，应包含该声明。参数值是包含 StringOrURI 的字符串，区分大小写。

ID 令牌可能包含其他声明(见 7.2.4.6、7.4.4.6 和附录 A)，未作规定的声明应忽略。

ID 令牌应签名，并可选择签名然后加密。如果 ID 令牌是加密的，它应先签名，然后加密，其结果是嵌套 JSON 令牌(见 8.2.4)。只有当响应类型中授权端点不返回 ID 令牌(例如使用授权码流程时)且依赖方注册时明确要求加密和签名算法参数〈alg〉值为 none 时，〈alg〉值才可以为 none，否则〈alg〉值不应为 none。

8.1.3 访问令牌

访问令牌是身份服务提供方发送给依赖方用于访问终端用户身份信息的凭据，代表着终端用户的授权。访问令牌中给出了用户信息的访问范围和访问有效期，访问范围和访问有效期由终端用户授权同意。访问令牌可作为提取授权信息的标识符；也可自包含授权信息，访问令牌中包含的授权信息可通过某种方式得到验证(例如数字签名)。

本标准要求授权服务器应先采用 SM3 算法(见 GB/T 32905—2016)对访问令牌进行杂凑运算，再使用 SM2 算法(见 GB/T 32918.2—2016)进行签名，最后使用 SM4 算法(见 GB/T 32907—2016)对其加密，将最后签名加密处理过的令牌发送出去。访问令牌包含了依赖方请求受保护资源所需的必要信息。

通常每种访问令牌类型都应有对应的规范文档。如果依赖方无法理解某访问令牌的类型，依赖方不应使用该访问令牌。

在传输和存储访问令牌时，应保证访问令牌的机密性。访问令牌的传输应使用 GM/T 0024—2014 定义的安全传输层协议。

当使用隐式许可流程进行授权时，访问令牌在 URI 片段中传输，但该传输方式可能将访问令牌暴露给未授权方。授权服务器应确保未授权方不能伪造和修改访问令牌，并且难以通过猜测访问令牌的方式产生有效的访问令牌。

依赖方应根据自身需求，请求最少的受保护资源访问范围的访问令牌。授权服务器应根据依赖方的身份，确定访问令牌的受保护资源访问范围，该访问范围不应高于依赖方请求的受保护资源访问范围。

本标准不规定资源服务器验证访问令牌有效性的方法。

为了防止访问令牌猜测攻击，授权服务器应保证攻击者猜测产生访问令牌的可能性应不高于 2^{-128}，宜不高于 2^{-160}。

8.1.4 刷新令牌

刷新令牌应用在访问令牌刷新机制中，由身份服务提供方发放给依赖方，用于在当前的访问令牌作

废或是过期时换取新的访问令牌，或是换取具有同等（或更小）作用域的另一个访问令牌（访问令牌的生存期和权限可以小于终端用户的授权范围）。

8.2 JSON 令牌

8.2.1 概述

JSON 令牌是一种 Javascript 对象符号，基于对安全令牌进行编码，实现身份信息和安全信息的跨安全域共享。JSON 令牌可以用来表示依赖方的请求参数，也可以用来表示终端用户的授权信息。令牌使用方可以对 JSON 令牌中包含的信息进行签名和（或）加密，如果同时进行签名和加密，则需要先签名后加密。

JSON 令牌用“.”分隔成不同含义的几个部分。JSON 令牌至少应包含三部分：

a) 第一部分是对 JSON 对象进行编码后形成的字符串：首先对 JSON 对象进行 UTF-8 编码，再进行 Base64url 编码。该 JSON 对象包含 JSON 令牌的签名和加密相关参数等信息，可包含以下成员：
   1) 成员名称：jwk[可选的]，JSON 令牌密钥（见 8.2.5）；
   2) 成员名称：jku[可选的]，JSON 令牌密钥 URL。
   第一部分还可包含其他的成员值（见 8.2.2 和 8.2.3）。
b) 第二部和第三部分因令牌的类型不同而有不同的定义（见 8.2.2 和 8.2.3）。

8.2.2 签名 JSON 令牌

签名 JSON 令牌包含三部分：

a) 第一部分除可包含 8.2.1 中定义的成员外，还应包含以下成员：
   1) 成员名称：alg[必选]，值为该签名 JSON 令牌的签名算法，该算法应在相对应的 JSON 令牌算法中，关于 JSON 令牌算法在本节描述；
   2) 成员名称：kid[必选]，值为该 JSON 令牌的密钥标识符，关于 JSON 令牌密钥的描述见 8.2.5。
b) 第二部分是对正文内容进行编码后的字符串：对正文内容先进行 UTF-8 编码，再进行 Base64url 编码后形成的字符串。
c) 第三部分是对正文内容的签名值进行编码后的字符串：首先使用第一部分所表示的 JSON 对象中 alg 指明的签名算法和相应 JSON 令牌密钥 kid 指明的签名密钥对正文内容进行签名，然后将该签名值进行 UTF-8 编码，再进行 Base64url 编码，最后形成字符串。JSON 令牌签名算法应支持 SM2 算法（见 GB/T 32918.2—2016）。

需要注意的是，如果 JSON 令牌没有签名和加密，则该 JSON 令牌第一部分的 alg 成员值为 none，且该令牌第三部分的值是空字符串。

8.2.3 加密 JSON 令牌

加密 JSON 令牌应包含三部分：

a) 第一部分除可包含 8.2.1 中定义的成员外，还应包含以下成员：
   1) 成员名称：alg[必选]，值为该加密 JSON 令牌的密钥加密算法，关于 JSON 令牌算法的描述见 8.2.6；
   2) 成员名称：kid[必选]，值为 JSON 令牌的密钥标识符，关于 JSON 令牌密钥的描述见 8.2.5；
   3) 成员名称：enc[必选]，值为该加密 JSON 令牌的正文加密算法。该算法应在相对应的

JSON 令牌算法中，关于 JSON 令牌算法的描述见 8.2.6。

除以上成员外，还可以包含其他与加密算法相关的成员参数，例如当采用椭圆曲线密码算法时，需要 epc、apu、apv 成员参数，关于这些参数的定义及使用不在本标准的规定范围。

b) 第二部分是对加密密钥进行编码后的字符串：该密钥用于加密正文内容，首先使用 JSON 令牌第一部分中成员 alg 指明的加密算法和相应 JSON 令牌密钥 kid 指明的密钥，对该加密密钥进行加密，再对密钥的密文进行 UTF-8 编码，最后再进行 Base64url 编码。

c) 第三部分是正文内容的密文以及相关加密参数，正文内容的密钥使用第二部分的加密密钥进行加密。该部分使用“.”分隔成几个部分，各个部分的内容与加密算法相关，例如，每个部分可以分别代表加密的初始化向量、附加值以及正文加密后的密文等内容，该部分的生成过程不在本标准的规定范围。JSON 令牌加密算法应支持 SM4 算法（见 GB/T 32907—2016）。

需要注意的是，如果 JSON 令牌没有签名和加密，则该 JSON 令牌第一部分的 alg 成员值为 none，且该令牌第三部分的值是空字符串。

8.2.4 嵌套 JSON 令牌

嵌套的 JSON 令牌是指把签名的 JSON 令牌当做加密 JSON 令牌的正文，即对要发放的内容先签名，然后加密。对应的接收方在收到该 JSON 令牌后应当先解密，再进行签名验证。

8.2.5 JSON 令牌密钥

JSON 令牌密钥是一个 JSON 对象，该 JSON 对象包含一个成员名称为 keys 的成员，该成员的值为 JSON 对象数组。该 JSON 对象数组的每个 JSON 对象元素表示一个密钥，每个 JSON 对象包含以下成员：

a) 成员名称：kty[必选]，表示该密钥的类型；

b) 成员名称：kid[必选]，表示该密钥的标识符；

c) 成员名称：k，表示对称密钥的值，在表示对称密钥时，该成员是必选的；

d) 其他各个类型密钥所需要的参数：参数名称作为成员名称，参数值作为成员值。

8.2.6 JSON 令牌算法

JSON 令牌算法是身份服务提供方或者依赖方所支持的密码算法，在各自的服务文档中应提供给开发者，具体实现不在本标准的规定范围，但身份服务提供方和依赖方应支持 SM2（见 GB/T 32918.2—2016）、SM3（见 GB/T 32905—2016）和 SM4 算法（见 GB/T 32907—2016），并且应该对 JSON 令牌的签名算法和加密算法加以区分。每个 JSON 令牌算法都有对应的杂凑算法，例如，签名 JSON 令牌的 alg 值为 SM3_SM2 时，表示使用杂凑算法为 SM3 的 SM2 签名算法，具体实现不在本标准的规定范围。

8.3 令牌安全保护要求

对于访问令牌、刷新令牌、ID 令牌等安全令牌的使用：身份服务提供方应防止非授权的泄漏和滥用，依赖方在使用的过程中应确保令牌信息的机密性，防止非授权的泄露。

身份服务提供方应采取以下方法防止令牌伪造和篡改：

a) 身份服务提供方对令牌进行数字签名。依赖方应验证数字签名，以确保该令牌由合法的身份服务提供方签发。

b) 利用 GM/T 0024—2014 中定义的安全通道来发送令牌。在本标准中，令牌都通过安全通道发送。这项措施只能对抗来自恶意第三方实体的攻击，并不适用于依赖方为攻击者的情况。

身份服务提供方应限制访问令牌的接收者范围和被访问的资源范围，即指明使用访问令牌来访问资源的实体身份（接收者）以及利用该访问令牌可访问资源的范围。可通过以下方式实现：在访问令牌

中包含访问者的标识符和被访问资源的范围，并可通过数字签名等方式确保这些信息不会被篡改或伪造。接收访问令牌的资源访问接口组件应验证该访问令牌的接收者列表中是否包含该依赖方的标识符。

身份服务提供方应对令牌使用设置时间戳和有效使用时间，以防止令牌重用。依赖方在使用令牌前，应检查时间戳和有效使用时间，以确保令牌是有效的。或者服务器可通过记录令牌的使用状态，并检查每个请求的状态，来防止令牌重用。

身份服务提供方应采取安全措施来防止令牌替换。令牌替换是指由恶意用户发起的、通过互换不同会话中的令牌来破坏鉴别流程的攻击，包括攻击者用其拥有的令牌替换合法用户的授权码。依赖方应能确定发放的ID令牌和访问令牌确实由该合法终端用户使用。如果没有采取此类安全措施，身份服务提供方不能使用隐式授权流程作为鉴别终端用户的方式。在本标准中，应利用ID令牌提供的机制预防令牌替换攻击：该ID令牌是被签名的安全令牌，并提供以下声明，包括iss(发布方)、sub(主体)、aud(接收方)、azp(授权方)、at_hash(访问令牌的杂凑值)和c_hash授权码的杂凑值等声明；其中，ID令牌的c_hash声明使依赖方能够防止授权码替换攻击，ID令牌的at_hash使依赖方能够防止访问令牌替换攻击。

本标准定义的令牌请求和令牌响应均使用GM/T 0024—2014中定义的安全通信协议，以检测并阻止数据包被重新排序。如果不使用SSLVPN技术规范 GM/T 0024—2014中定义的安全通信协议，则需使用其他安全机制。在隐式鉴别流程中，访问令牌应通过HTTPS协议传输，通过添加到依赖方的redirect_uri的片段部分返回。

针对刷新令牌，在授权过程中，授权服务器应明确标识出刷新令牌是用于长期许可，并给出刷新令牌的有效使用时间。授权服务器应该提供一种机制，使得终端用户可以取消授权给依赖方的访问令牌和刷新令牌。

9 用户信息访问

9.1 声明的类型

9.1.1 概述

声明是由身份服务提供方生成的关于实体的数据，可用于表述用户的身份属性信息。通过传递声明，身份服务提供方向依赖方提供终端用户身份信息。

本标准定义三种声明类型：

a) 规范性声明 Normal Claims

身份服务提供方直接宣称、支持和理解的声明；

b) 聚合式声明 Aggregated Claims

由除了身份服务提供方外的其他声明提供方宣称的声明，但声明由身份服务提供方返回；

c) 分布式声明 Distributed Claims

由除了身份服务提供方外的其他声明提供方宣称的声明，但由身份服务提供方返回该声明的引用。

身份服务提供方应支持 Normal Claims。可以选择性地支持 Aggregated Claims 和 Distributed Claims 声明。

9.1.2 规范性声明

规范性声明使用JSON对象中的一个成员来表示。声明名称作为成员名称，声明值作为成员值。该规范定义了一组规范性声明集合(见附录A)。他们可以在用户信息响应中返回(见9.3.3)，或在ID令牌中返回(见8.1.2)。

9.1.3 聚合式声明和分布式声明

聚合式声明和分布式声明使用 JSON 对象来表示，该 JSON 对象包含了声明的内容，并应包含_claim_names 和_claim_sources 这两个特殊的成员：

a) 成员名称：_claim_names

该成员值是 JSON 对象，聚合式声明或分布式声明类型的声明名称是该 JSON 对象所包含成员的成员名称。JSON 对象中的每一个成员值是一个引用名称，该引用名称是_claim_source 中的成员名，根据_claim_sources 的成员名对应的成员值可以提取出实际的声明值。

b) 成员名称：_claim_sources

该成员值是 JSON 对象，该 JSON 对象所包含成员的成员名称是_claim_names 成员的成员值引用，其成员值包含几组聚合式声明或分布式声明类型声明的引用。成员值可以有以下格式之一，取决于它是否支持聚合式声明或分布式声明：

1) 聚合式声明类型

该成员值是 JSON 对象，该 JSON 对象应包含一个成员，该成员值是一个 JSON 令牌，该 JSON 令牌应包含_claim_names 成员值中引用的所有声明。该 JSON 对象也可以存在其他成员，所使用的任何不被理解的成员应被忽略。

成员名称：JWT[必选]

包含声明的 JSON 令牌。

该 JSON 令牌不应包含 sub 声明，除非它的值在声明提供方处是一个终端用户(而不是身份服务提供方或其他实体)的标识符。这通常意味着不应提供 sub 声明，以避免终端用户标识符直接暴露。

本标准给出一个聚合式声明的示例：

```
{
"name":"Jane Doe",
"given_name":"Jane",
"family_name":"Doe",
"birthdate":"0000-03-22",
"eye_color":"blue",
"email":"janedoe@example.com",
"_claim_names":{
"address":"src1",
"phone_number":"src1"
},
"_claim_sources":{
"src1":{"JWT":"jwt_header.jwt_part2.jwt_part3"}
}
}
```

2) 分布式声明类型

该成员值是一个 JSON 对象，它包含以下成员：

成员名称：endpoint[必选]

可以检索相关的声明的资源端点。端点的 URL 应以 JSON 令牌形式返回声明。

成员名称：access_token[可选]

能够用来从端点 URL 检索声明的访问令牌。声明应通过授权请求报头字段请求，并且声明提供方应支持此方法。如果访问令牌不可用，依赖方可能需要另外获取访问令牌，或使用与声明提供方预先

商定的访问令牌，或声明提供方重新验证终端用户和(或)重新授权依赖方。

不应从声明提供方返回一个 sub(主体)声明，除非它的值在声明提供方处是一个终端用户(而不是身份服务提供方或其他实体)的标识符。

通常，身份服务提供方适合使用 Aggregated Claims 和 Distributed Claims。关于什么时候使用什么类型，应由具体的依赖方与身份服务提供方协商决定，不在本标准的规定范围。

9.2 语言和文字声明

声明值及其引用值的表示方法应能够支持多种语言和文字。为了指定声明值所使用的语言和文字，应该在成员名称中添加 RFC 5646 定义的语言标记，使用“#”字符分隔。例如，FAMILY_NAME#zh-CN 表示了中文描述的姓氏。又如，声明值 website 和 website#zh，分别表示未指定语言的网址和中文网址。

声明名称应区分大小写。通常语言类型拼写用小写字符，地区名称的拼写用大写字符，文字类型的拼写用大小写混合的字符。

身份服务提供方应尽量匹配依赖方所要求的用于表示声明的语言环境。身份服务提供方应尽量处理复杂的语言标记匹配，不应将此类复杂的事务转移给依赖方处理。

本标准定义了如下的授权请求参数，依赖方使用这些参数来指定即将返回的声明所首选的语言和文字：

〈claims_locales〉[可选]

终端用户首选的语言和文字，用 RFC 5646 定义的语言标签值列表表示，并以空格分隔，按照偏好排序。如果身份服务提供方不支持某些要求的语言环境或全部都不支持，不应导致错误。

9.3 用户信息端点

9.3.1 概述

用户信息端点是用于返回受保护资源的端口，返回已经通过鉴别的终端用户身份属性的声明。如果想获得关于终端用户身份属性的声明，依赖方需要向用户信息端点呈递请求，并在请求中携带在此会话中从身份服务提供方处获得的访问令牌。这些声明通常是由包含声明名称和值的 JSON 对象返回。

与用户信息端点的通信应使用 GM/T 0024—2014 中定义的安全通信协议。

用户信息端点应支持使用 HTTP GET 和 HTTP POST 方法。

用户信息端点应可以接受依赖方与授权服务器协商的访问令牌类型。

用户信息端点应支持跨域资源共享或其他适用的方法，以使 Java 脚本依赖方可以访问该端点。

9.3.2 用户信息请求

依赖方使用 HTTP GET 或 HTTP POST 方法向用户信息端点发送请求。请求中发送的访问令牌应是依赖方与授权服务器协商好的访问令牌类型。

建议请求使用 HTTP GET 方法，并将访问令牌作为 Authorization 发送。

9.3.3 用户信息成功响应

用户信息声明应作为一个 JSON 对象的成员返回，除非客户注册时要求签名和(或)加密响应。可以返回附录 A 中定义的声明，也可以返回没有在本标准中定义的扩展的声明。

出于保护隐私的原因，身份服务提供方可以选择不返回一些要求的声明值。

如果某声明没有返回，该声明的名称应该从 JSON 对象去除，它不应该以 null 值或空字符串值返回。

sub 声明应始终在用户信息响应中返回。

注：由于存在令牌替换攻击的可能性，用户信息响应不能作为由 ID 令牌的 sub 参数值确定的终端用户的鉴别信息。本次响应的 sub 参数值应与 ID 令牌的 sub 声明相匹配，否则不能使用该用户信息响应。

用户信息端点应在 Content-Type 头中指示返回的格式。如果响应主体是文本的 JSON 对象，HTTP 响应内容类型应为 application/ json，响应主体应该使用 UTF-8 编码。

如果对用户信息响应进行签名和(或)加密，那么返回的声明使用 JSON 令牌格式，并且内容类型应是 application/jwt。该响应可能只进行加密而没有签名。如果同时要求签名和加密时，JSON 令牌应先签名后再加密，其结果是一个嵌套的 JSON 令牌。

如果签名，用户信息响应应包含 iss 声明和 aud 声明。iss 声明值应该是发布方的标识符 URL。aud 值应为(或包含)依赖方的 client_id。

用户信息响应通常包含个人身份信息。因此，对指定用途信息的发布应按照相关规范在鉴别时或鉴别前获得终端用户的同意。

依赖方应只存储需要的用户信息数据，且应使接收到的数据与使用目的相关联。

9.3.4 用户信息错误响应

当错误情况发生时，用户信息端点返回错误响应。对于不同类型的访问令牌，错误响应的参数由该访问令牌类型的说明文档说明，不在本标准的规定范围。

9.3.5 用户信息响应验证

依赖方应按如下步骤验证用户信息响应：

a) 根据 RFC 6125 定义的 TLS 服务器证书验证规则，验证返回用户信息的身份服务提供方确实是目的身份服务提供方；

b) 如果依赖方在注册过程中提供一个〈userinfo_encrypted_response_alg〉参数，使用注册时该参数指定的解密密钥解密用户信息响应；

c) 如果响应被签名，客户应根据签名 JSON 令牌验证签名。

9.4 用户信息请求声明

9.4.1 使用范围值请求声明

依赖方使用〈scope〉参数来指定访问令牌的权限，用于说明访问令牌相关联的权限指定的可访问的资源范围。受保护的资源端点可以根据所使用的参数来执行相应的操作并返回信息(如根据〈scope〉参数返回指定范围的受保护资源)。如果使用值传递的方式传递参数及参数值，鉴别请求中的 scope 参数必须包含 openid 值，例如，请求中包含“scope”:“openid”。

对于本标准定义的协议，范围值可以用来请求特定的声明值。

通过以下〈scope〉参数值请求的声明可以被授权服务器视为自选声明。

本标准定义了以下〈scope〉参数值用于请求声明：

a) 〈profile〉[可选]

这个范围值请求访问终端用户的默认配置声明，其中有：〈name〉、〈family_name〉、〈given_name〉、〈middle_name〉、〈nickname〉、〈preferred_username〉、〈profile〉、〈picture〉、〈website〉、〈gender〉、〈birthdate〉、〈zoneinfo〉、〈locale〉和〈updated_at〉。

b) 〈email〉[可选]

这个范围值请求访问〈email〉和〈email_verified〉声明。

c) 〈address〉[可选]

这个范围值请求访问〈address〉声明。

d) 〈phone〉[可选]

这个范围值请求访问〈phone_number〉和〈phone_number_verified〉声明。

多个范围值可以用空格分隔的列表形式表示，用 ASCII 码表示，区分大小写。

当〈response_type〉参数值使得身份服务提供方发放访问令牌，则通过〈profile〉，〈email〉，〈address〉和〈phone〉范围值请求的声明是从用户信息端点返回的(见 9.3.3)。然而，当没有访问令牌发放(这对应于〈response_type〉的值为 id_token 的情况下)，该请求所请求的声明是在 ID 令牌中返回的。

在某些情况下，终端用户不允许身份服务提供方提供给依赖方所请求的部分或全部信息。为了尽量减少终端用户的信息泄漏，依赖方可以选择向用户信息端点只请求用户信息的子集。

9.4.2 使用〈claims〉请求参数请求声明

9.4.2.1 授权请求参数

本标准定义了如下的授权请求参数，依赖方可以使用这些参数来请求特别的声明：

〈claims〉[可选]

此参数用来请求返回特定的声明。该值是一个列出请求的声明的 JSON 对象。

如果鉴别请求中包含〈claims〉参数，表示请求从用户信息端点和(或)在 ID 令牌中返回特定的声明。该参数值是含有被请求的声明列表的 JSON 对象。被请求的声明的属性也可以在该参数中指定。

该参数是可选的。如果身份服务提供方不支持该参数而依赖方使用了该参数，则身份服务提供方应给依赖方返回一组它认为对依赖方有用的、身份服务提供方推断终端用户认为是合适的声明。身份服务提供方在服务文档中使用〈claims_parameter_supported〉参数用来表明身份服务提供方是否支持该参数。

〈claims〉参数值在请求中用 UTF-8 编码的 JSON 对象来表示。当使用请求对象发起请求时，如附录 B 中所述，该 JSON 对象作为请求对象中成员名称为〈claims〉的成员值。

上述 JSON 对象的成员如下：

a) 〈userinfo〉[可选]

请求从用户信息端点返回的声明的列表。如果使用该参数，请求的声明列表加入到使用〈scope〉参数值请求的声明列表中。如果不使用该参数，从用户信息端点请求的声明只有〈scope〉参数值要求的声明。

当〈userinfo〉成员使用时，鉴别请求的〈response_type〉的参数值应使依赖方能够收到一个访问令牌，依赖方用该访问令牌向用户信息端点发出请求。

b) 〈id_token〉[可选]

请求列出的声明在 ID 令牌中返回。如果使用该参数，请求的声明列表要加入到在 ID 令牌的默认声明列表中。如果不使用该参数，则默认请求 ID 令牌，即按照 ID 令牌的定义(见 8.1.2)和 7.2.4.6、7.3.3.10、7.4.3.11 及 7.4.4.6 中所述的各个流程中定义的声明进行请求。

也可能有其他成员。应忽略所有不能被理解的成员。

需要注意当请求的声明不属于附录 A 定义的规范性声明时，例如请求 http://example.info/claims/groups 声明。这种情况下使用〈claims〉参数是请求标准声明之外的声明的唯一方法。该参数也是请求标准声明特定组合的唯一方法。

9.4.2.2 〈claims〉参数的成员值

〈claims〉参数的 userinfo 和 id_token 请求成员的成员值都是 JSON 对象，且该 JSON 对象的成员由声明的名字作为成员名，成员值应是下列之一：

a) null

表明该声明使用默认的请求方式。需要说明的是，该值表明此声明为自选声明。例如，以下声明

请求：

"given_name":null

该声明请求表示以默认的方式请求 given_name 声明。

b) JSON 对象

用于提供有关被请求的声明的附加信息。本标准对该 JSON 对象定义了以下成员：

1) 〈essential〉[可选]

表示被请求的声明是否是必要的声明。如果该成员值为 true，则表明声明是一个必要的声明。例如，以下声明请求：

"auth_time":{"essential":true}

该声明请求表示返回 auth_time 声明是必要的。

如果该成员值为 false，则表明它是自选声明。该成员值默认为 false。

通过请求声明作为必要声明，依赖方可以告知终端用户这些声明以确保终端用户所要求的特定任务的顺利授权。请注意，即使由于终端用户并没有授权这些声明或者它们不存在，使得声明不可用，当声明返回时授权服务器也不能产生错误，无论是必选还是自选，除非另有具体的要求规定。

2) 〈value〉[可选]

请求该声明由一个特定的值返回。例如以下声明请求：

"sub":{"value":"248289761001"}

以上例子可用于指定主体标识符为 248289761001 的终端用户适用于该次请求。

〈value〉的取值应为请求声明的有效值。在个体声明的定义中，可以对如何使用以及何时使用〈value〉值进行限定。

3) 〈values〉[可选]

该声明通常表示为一组声明值，在请求中使用该参数表示身份服务提供方可以返回该组值中的任意一个，并且声明值在组内的顺序按照该组值常用的或自选的排列顺序。

该数组中的值应是被请求的声明的有效值。在个体声明的定义中，可以对如何使用以及何时使用〈value〉值进行限定。

可以定义其他成员来提供有关声明请求的附加信息。应忽略所有不能被理解的成员。

9.4.2.3 请求“acr”声明

如果 acr 声明作为 ID 令牌的基本声明，用某参数值请求特定的身份鉴别上下文类的引用值，并且实现支持该声明参数，授权服务器应返回一个 acr 声明值，并且该值与请求中的值相匹配。授权服务器可能对终端用户再次使用附加的因素重新鉴别，从而满足该需求。如果这是一个基本声明但是不满足需求，授权服务器应将此次请求作为失败的鉴别请求。

注意，依赖方可能会使用 acr_values 请求参数或使用不包含"essential":true 的单独的 acr 声明请求，从而将 acr 请求作为自选声明。如果声明不是基本声明并且不能提供请求的参数值，授权服务器应该将会话的当前 acr 值作为 acr 声明返回。如果声明不是基本声明，授权服务器不需要在它的响应中返回该声明。

9.5 声明的稳定性和唯一性

一起使用的 sub 声明和 iss 声明，是依赖方可以用来确定终端用户的一组唯一的稳定的标识符声明(见 8.1.2)，因为 sub 声明应分配给(且不重新分配)一个特定的终端用户。因此，对于一个给定的终端终用户，唯一的标识符是 iss 声明和 sub 声明的组合。

其他声明不能保证产生如上作用。例如，发布方可以在不同的端点为不同的终端用户重复使用相同的 email 声明值，并且作为声明的 email 地址对于一个给定的终端用户可能会随时间而改变。因此，

其他的声明，如 email、phone_number 和 preferred_username 不能被用作唯一标识终端用户的标识符。

10 签名和加密要求

10.1 概述

为了确保消息的完整性和来源的真实可靠性，加密和签名应满足：

a) 应采用签名 JSON 令牌方式和加密 JSON 令牌方式对 ID 令牌、用户信息响应、请求对象和依赖方身份鉴别数据等内容分别进行签名和加密；

b) 当同时对消息进行签名和加密时，应先签名再加密，加密后的结果是一个嵌套 JSON 令牌；

c) 所有 JSON 令牌采用的加密方法中，都应进行完整性检查。

由身份服务提供方公布其支持的签名和加密算法，也可以通过其他方式提供这些信息。由依赖方在注册请求中声明其需要的签名和加密算法，或者可以通过其他方式向身份服务提供方传达此信息。

由身份服务提供方发布其公开密钥，也可以通过其他方式提供这些信息。由依赖方通过其注册请求公布其公开密钥，或者可以通过其他方式向身份服务提供方传达此信息。

10.2 签名

10.2.1 签名算法

为了确保请求参数在传递的过程中没有被篡改，依赖方和身份服务提供方需要对请求或响应中的敏感内容进行签名。

签名方应选择消息接收者所支持的签名算法，包括以下两种类型的签名算法：

a) 非对称签名算法

当使用诸如 SM2 的非对称算法签名时，JSON 令牌第一部分的〈alg〉参数值应是一个在 JSON 令牌算法中定义的算法。用来对内容签名的私钥应与发送方在其 JSON 令牌密钥文件中发布的用于签名验证的公钥相关联。如果 JSON 令牌密钥文件中引用有多个密钥，应在 JSON 令牌的第一部分提供一个密钥标识符〈kid〉参数值。使用的密钥应支持签名。

b) 对称签名算法

当采用基于 MAC 的签名时，JSON 令牌第一部分的〈alg〉参数值应是一个在 JSON 令牌算法中定义的 MAC 算法。所使用的 MAC 密钥是依赖方口令〈client_secret〉参数值的 UTF-8 编码表示的八位位组，〈client_secret〉参数值应具备足够的熵以预防猜测攻击。无保密能力型依赖方不能使用对称签名。

10.2.2 非对称签名密钥更新

签名方可以通过以下方法完成签名密钥的更新：

a) 签名方应在 JSON 令牌密钥集合的 jwks_uri 指向的位置中公布其公钥，并且应在每个消息的 JSON 令牌第一部分的〈kid〉参数指明用来验证签名的密钥信息。签名方可以通过在 JSON 令牌密钥集合的 jwks_uri 指向的位置中，定期添加新密钥来更新旧的密钥。签名方可以根据自己的判定开始使用新的密钥，并且通过〈kid〉参数来通知验证者；

b) 验证方在收到一个陌生的〈kid〉参数值时，应回到公布 JSON 令牌密钥集合的位置重新检索密钥；

c) JSON 令牌密钥集合的 jwks_uri 指向的位置，应在一段合理的时间内保留最近丢弃的签名密钥。

10.3 加密

10.3.1 加密算法

为了防止协议消息中涉及的敏感信息泄露，协议参与方需要对协议消息进行加密。

加密方应选择接收方所支持的加密算法，包括以下两类加密算法：

a） 非对称加密算法：SM2（见 GB/T 32918.4—2016）

一般采用非对称加密算法来进行密钥协商，所协商的密钥是一个对称密钥，用于对签名 JSON 令牌进行加密。加密方应从接收方公布的 JSON 令牌密钥集合文件中选择一个公钥，用于加密所协商的密钥。如果在 JSON 令牌密钥集合中有多个引用的密钥，JSON 令牌第一部分中应包含〈kid〉参数值，该参数用来指明所使用的具体公钥。该过程中使用的密钥应支持加密。

b） 对称加密

对称加密密钥通过计算〈client_secret〉参数值产生，先将〈client_secret〉参数值进行 SM3 杂凑运算，将杂凑值的 UTF-8 表示的八位位组取左边的一半作为密钥。其中无保密能力的依赖方不应使用对称加密。

10.3.2 非对称加密密钥的更新

非对称加密密钥的更新要求如下：

a） 加密密钥的更新与签名密钥的更新过程不同，加密密钥的更新由解密方执行，不能依靠〈kid〉参数的变化作为需要改变的信号；

b） 加密方首先应从接收方的 jwks_uri 位置提供的 JSON 令牌密钥集合中选择合适的密钥；

c） 加密方应使用在 JSON 令牌第一部分中的〈kid〉头参数告知解密方：用于解密的私钥具体是接收方 JSON 令牌密钥集合中哪一个位置对应的密钥；

d） 更新密钥时，解密方应在其 jwks_uri 位置发布新的密钥，并从 JSON 令牌密钥集合中删除不再使用的密钥。如[RFC2616]中定义，该 jwks_uri 应在响应中包括一个包含 max-age 指令的 Cache-Control 头，使加密方可以安全缓存 JSON 令牌密钥集合，而不必为每一个加密的事件重新检索文档。解密方应从 jwks_uri 指向的 JSON 令牌密钥集合中删除不适用的密钥，但在合理的时间内保留他们，配合缓存持续时间，允许加密方在一段时间里获得新密钥，以实现密钥之间的平滑过渡。

10.4 对称密钥的熵

密钥由依赖方口令 client_secret 值推导计算而来。因此，使用对称密码算法进行签名和加密操作时，client_secret 值应包含足够的熵以便产生符合算法强度要求的密钥。此外，client_secret 值也应符合特定算法对 MAC 密钥的要求。

10.5 签名和加密的顺序

为了确保完整性和不可抵赖性，本标准要求对明文的 JSON 令牌进行签名。如果同时需要签名和加密，应先签名后加密，从而得到一个嵌套 JSON 令牌。需要注意的是，因为所有的 JSON 令牌加密算法都提供完整性保护，因此没有必要对加密的内容单独签名。

附 录 A
（规范性附录）
规范性声明

该规范定义了一组标准的基础声明集合。他们可以在用户信息响应中返回（见 9.3.3），或在 ID 令牌中返回（见 8.1.2）。

表 A.1 规范性声明列表

声明名称	类型	描述
sub	字符串	终端用户在发放方的主体标识符
name	字符串	可显示的终端用户的全名，包括其名称的所有部分
given_name	字符串	终端用户的名字。注意：某些情况下，一个人可以有多个名字；所有的名字可用空格分隔的字符串表示出来
family_name	字符串	终端用户的姓氏。注意：某些情况下，一个人可以有多个姓氏或没有姓氏；所有的姓氏可用空格分隔的字符串表示出来
middle_name	字符串	终端用户的中间名字。注意：某些情况下，一个人可以有多个中间名字或没有中间名字；所有的中间名字都可以用空格分隔的字符串表示出来
nickname	字符串	终端用户的昵称。可能和终端用户名字相同，也可能不同
preferred_username	字符串	终端用户希望在依赖方使用的速记名字。该值可能是包含特殊字符（例如，“@”“/”或者空格）的有效 JSON 字符串。依赖方不能依赖该值唯一标识终端用户（见 9.5）
profile	字符串	描述终端用户基本信息的网页的 URL。该网页的内容应该与终端用户相关
picture	字符串	终端用户图片文件的 URL。该 URL 应指向描述终端用户图片文件（例如，PNG、JPEG 或者 GIF 等格式的终端用户的头像文件），而不是包含图片文件的网页。注意：该 URL 应该指向可以描述终端用户的图片，而不是终端用户随意上传的图片
website	字符串	终端用户的个人网页或者博客的 URL
email	字符串	终端用户的首选电子邮件地址，该值应符合标准的电子邮件表示语法（RFC 5322 定义的 addr-spec 语法），不能依赖该值唯一确定终端用户的身份（见 9.5）
email_verified	布尔值	如果终端用户的电子邮件已经通过验证，则该值为 true，否则为 false。当该声明值为 true 时，意味着身份服务提供方已经采取措施确定该电子邮件地址是该终端用户使用的邮件地址。验证电子邮件地址的方法是上下文已经确定的
gender	字符串	终端用户的性别

表 A.1（续）

声明名称	类型	描述
birthdate	字符串	终端用户的生日，采用 ISO 8601:2004 定义的 YYYY-MM-DD 格式。年份的值可能省略，表示为 0000。如果只显示年份，则使用 YYYY 格式。需要注意根据底层平台的日期相关的函数，只提供年份可能会产生不同的月份和日期，实现者应注意该因素，正确处理日期
zoneinfo	字符串	用来表示终端用户所在时区的字符串，例如，Asia/China 或者 America/Los_Angeles
locale	字符串	终端用户所在的区域，用 RFC 5646 中的语言标记来表示。通常是用破折号连接一个 ISO 639-1 Alpha-2（见 ISO 639-1）定义的小写的语言代码和一个 ISO 3166-1 Alpha-2（ISO 3166-1）定义的大写的国家代码，也可用下划线代替破折号，例如 en_CN
phone_number	字符串	终端用户的首选电话号码，该声明使用 E.164 定义的格式，例如，+1 (425)555-1212 或者 +56 (2)687 2400。如果电话号码有分机，那么使用 RFC 3966 中的定义，例如+1 (604)555-1234;ext=5678
phone_number_verified	布尔值	如果电话号码经过验证，则为 true，否则为 false。当该声明值为 true 的时候，意味着身份服务提供方已经采取措施确定该电话号码是该终端用户使用的。验证电话号码的方法是上下文已经确定的。当为 true 时，电话号码的格式应符合 E.164 定义的格式，并且有分机时应表示为 RFC 3966 定义的格式
address	JSON 对象	终端用户首选的邮递地址，address 的值是 RFC 4627 标准定义的 JSON 结构
updated_at	数字	终端用户最近一次更新用户信息的时间，它的值是一个 JSON 数字，该数字代表自 1970 年 1 月 1 日 0 时 0 分 0 秒(1970-01-01T0:0:0Z) UTC 至更新的时间的秒数

附 录 B
（资料性附录）
身份服务提供方的基础配置

身份服务提供方应配置以下必选信息，并在其服务文档中对以下所述的配置信息给予说明：

a) 发布方标识符(issuer_identifier)[必选]；
b) 授权端点 URL(authorization_endpoint)[必选]；
c) 令牌端点 URL(token_endpoint)[必选]；
d) 用户信息端点 URL(userinfo_endpoint)[推荐]相关内容见 9.3；
e) JSON 令牌密钥 URI(jwks_uri)[必选]，相关内容见 8.2.5；
f) 支持的可访问的资源范围值(scopes_supported)[推荐]
可访问的资源范围值 scope 相关内容见 9.4.1；
g) 支持的响应类型(response_types_supported)[必选]
响应类型见第 7 章；
h) 支持的响应模式(response_modes_supported)[可选]
响应模式见第 7 章；
i) 支持的授权类型(grant_types_supported)[可选]
授权类型在本标准不作规定；
j) 支持的 ID 令牌签名算法(id_token_signing_alg_values_supported)[必选]
ID 令牌签名算法相关内容见 8.2.6 和 10.2；
k) 支持的 ID 令牌密钥加密算法(id_token_encryption_alg_values_supported)[可选]
ID 令牌密钥加密算法相关内容见 8.2.6 和 10.3；
l) 支持的 ID 令牌正文加密算法(id_token_encryption_enc_values_supported)[可选]
ID 令牌正文加密算法相关内容见 8.2.6 和 10.3；
m) 支持的用户信息签名算法(userinfo_signing_alg_values_supported)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；
n) 支持的用户信息密钥加密算法(userinfo_encryption_alg_values_supported)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；
o) 支持的用户信息正文加密算法(userinfo_encryption_enc_values_supported)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；
p) 支持的请求对象签名算法(request_object_signing_alg_values_supported)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；
q) 支持的请求对象密钥加密算法(request_object_encryption_alg_values_supported)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；
r) 支持的请求对象正文加密算法(request_object_encryption_enc_values_supported)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；
s) 支持的令牌端点鉴别签名算法(token_endpoint_auth_signing_alg_values_supported)[可选]
本标准不作规定；
t) 支持的显示模式(display_values_supported)[可选]
显示模式见 7.2.3.1；
u) 支持的声明类型(claim_types_supported)[可选]
声明类型见 9.1；

v) 支持的声明(claims_supported)[可选]
声明见第9章；
w) 服务文档URL(service_documentation)[可选]
身份服务提供方的服务文档的引用；
x) 支持的声明的语言及脚本(claims_locales_supported)[可选]
声明的语言及脚本见9.2；
y) 支持的语言及脚本(ui_locales_supported)[可选]
语言及脚本见9.2；
z) 是否支持claims参数(claims_parameter_supported)[可选]
布尔值，指示该服务器对〈claims〉参数的支持情况。claims参数的描述见9.4.2；
aa) 身份服务提供方提供给依赖方的注册指南URL(op_policy_uri)[可选]
身份服务提供方的注册指南的URL地址；
bb) 在依赖方注册时显示给依赖方的身份服务提供方服务条款URL(op_tos_uri)[可选]
身份服务提供方的服务条款的URL地址。

注：本标准不对以上配置信息的具体实现进行规定。

附 录 C
（资料性附录）
依赖方的注册信息

依赖方的注册信息如下：

a） 重定向 URL 地址(redirect_uris)[必选]；

b） 响应类型(response_types)[可选]
响应类型见本标准附录 B；

c） 授权类型(grant_types)[可选]；

d） 应用类型(application_type)[可选]；

e） 联系方式(contacts)[可选]
依赖方的联系方式；

f） 依赖方名称(client_name)[可选]
依赖方的名称；

g） logo URI(logo_uri)[可选]
依赖方的 LOGO 图标的 URL 地址；

h） 依赖方主页 URL(client_uri)[可选]
依赖方主页的 URL 地址；

i） 依赖方信息说明(policy_uri)[可选]
依赖方信息说明的 URL 地址；

j） 依赖方服务条款(tos_uri)[可选]
依赖方的服务条款的 URL 地址；

k） JSON 令牌密钥 URI(jwks_uri)[可选]
JSON 令牌密钥见 8.2.5；

l） JSON 令牌密钥(jwks)[可选]
JSON 令牌密钥见 8.2.5；

m） ID 令牌签名响应算法(id_token_signed_response_alg)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

n） ID 令牌密钥加密响应算法(id_token_encrypted_response_alg)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

o） ID 令牌正文加密响应算法(id_token_encrypted_response_enc)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

p） 用户信息签名响应算法(userinfo_signed_response_alg)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

q） 用户信息密钥加密响应算法(userinfo_encrypted_response_alg)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

r） 用户信息正文加密响应算法(userinfo_encrypted_response_enc)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

s） 请求对象签名算法(request_object_signing_alg)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

t） 请求对象密钥加密算法(request_object_encryption_alg)[可选]
JSON 令牌算法相关内容见 8.2.6 和第 10 章；

u) 请求对象正文加密算法(request_object_encryption_enc)[可选]

JSON 令牌算法相关内容见 8.2.6 和第 10 章;

v) 令牌端点鉴别方案(token_endpoint_auth_method)[可选];

w) 令牌端点鉴别签名算法(token_endpoint_auth_signing_alg)[可选];

x) 默认最大鉴别有效期(default_max_age)[可选]

最大鉴别有效期见 7.2.3.1;

y) 在 ID 令牌中是否需要鉴别时间声明(require_auth_time)[可选]

布尔值,确定在 ID 令牌中是否包含鉴别时间的声明。鉴别时间声明见 8.1.2。

以上配置信息的具体实现不属于本标准的规定范围。本标准假定依赖方已经获得了足够的凭据并且向身份服务提供方提供了必需的信息。该过程可以通过动态注册或者其他方式实现,本标准不对具体实现过程进行规定。

参 考 文 献

[1] International Organization for Standardization,"ISO 639-1:2002.Codes for the representation of names of languages—Part 1:Alpha-2 code," 2002.

[2] Jones,M.,"JSON Web Algorithms (JWA)," draft-ietf-jose-json-web-algorithms (work in progress),November 2013 (HTML).

[3] Jones,M.,Rescorla,E.,and J.Hildebrand,"JSON Web Encryption (JWE)," draft-ietf-jose-json-web-encryption (work in progress),November 2013 (HTML).

[4] Jones,M.,"JSON Web Key (JWK)," draft-ietf-jose-json-web-key (work in progress),November 2013 (HTML).

[5] Jones,M.,Bradley,J.,and N.Sakimura,"JSON Web Signature (JWS)," draft-ietf-jose-json-web-signature (work in progress),November 2013 (HTML).

[6] Jones,M.,Bradley,J.,and N.Sakimura,"JSON Web Token (JWT)," draft-ietf-oauth-json-web-token (work in progress),November 2013 (HTML).

[7] Campbell,B.,Mortimore,C.,Jones,M.,and Y.Goland,"Assertion Framework for OAuth 2.0 Client Authentication and Authorization Grants," draft-ietf-oauth-assertions (work in progress),December 2013 (HTML).

[8] Jones,M.,Campbell,B.,and C.Mortimore,"JSON Web Token (JWT)Profile for OAuth 2.0 Client Authentication and Authorization Grants," draft-ietf-oauth-jwt-bearer (work in progress),December 2013 (HTML).

[9] de Medeiros,B.,Ed.,Scurtescu,M.,Tarjan,P.,and M.Jones,"OAuth 2.0 Multiple Response Type Encoding Practices," February 2014.

[10] Sakimura,N.,Bradley,J.,Jones,M.,and E.Jay,"OpenID Connect Discovery 1.0," February 2014.

[11] Sakimura,N.,Bradley,J.,and M.Jones,"OpenID Connect Dynamic Client Registration 1.0," February 2014.

[12] Dierks,T.and C.Allen,"The TLS Protocol Version 1.0," RFC 2246,January 1999 (TXT).

[13] Crockford,D.,"The application/json Media Type for JavaScript Object Notation (JSON)," RFC 4627,July 2006 (TXT).

[14] Hardt,D.,"The OAuth 2.0 Authorization Framework," RFC 6749,October 2012 (TXT).

[15] Lodderstedt,T.,McGloin,M.,and P.Hunt,"OAuth 2.0 Threat Model and Security Considerations," RFC 6819,January 2013 (TXT).

[16] Sakimura,N.,Bradley,J.,Jones,M.,de Medeiros,B.,and C.Mortimore,"OpenID Connect Basic Client Implementer's Guide 1.0," February 2014.

[17] Sakimura,N.,Bradley,J.,Jones,M.,de Medeiros,B.,and C.Mortimore,"OpenID Connect Implicit Client Implementer's Guide 1.0," February 2014.

[18] Sakimura,N.,Bradley,J.,Jones,M.,de Medeiros,B.,Mortimore,C.,and E.Jay,"OpenID Connect Session Management 1.0," February 2014.

[19] International Telecommunication Union,"ITU-T Recommendation X.1252—Cyberspace security—Identity management—Baseline identity management terms and definitions," ITU-T X.1252,November 2010.

中华人民共和国密码
行业标准
开放的身份鉴别框架
GM/T 0069—2019
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 3 字数 90 千字
2019年10第一版 2019年10第一次印刷
*
书号:155066·2-34574 定价 54.00 元

GM/T 0069-2019