



# 中华人民共和国国家标准

GB/T 47475—2026

## 网络安全技术 开放的第三方资源授权协议

Cybersecurity technology—Open resource authorization protocol for third party

2026-04-30 发布

2026-11-01 实施

国家市场监督管理总局  
国家标准化管理委员会 发布



目 次

前言 ..... III

引言 ..... IV

1 范围 ..... 1

2 规范性引用文件 ..... 1

3 术语和定义 ..... 1

4 缩略语 ..... 3

5 通则 ..... 3

    5.1 协议角色 ..... 3

    5.2 协议基本流程 ..... 3

    5.3 协议端点类型 ..... 4

6 客户端类型和要求 ..... 5

    6.1 类型 ..... 5

    6.2 标识符 ..... 5

    6.3 注册 ..... 6

    6.4 身份鉴别 ..... 6

7 授权流程 ..... 7

    7.1 授权许可类型 ..... 7

    7.2 授权码许可 ..... 7

    7.3 客户端身份凭据许可 ..... 11

    7.4 设备授权许可 ..... 12

8 令牌发放与刷新 ..... 14

    8.1 令牌类型 ..... 14

    8.2 访问令牌发放 ..... 15

    8.3 访问令牌刷新 ..... 16

9 受保护资源访问 ..... 18

    9.1 受保护资源访问 ..... 18

    9.2 成功响应 ..... 18

    9.3 出错响应 ..... 18

附录 A (资料性) 协议参数说明 ..... 19

    A.1 参数说明 ..... 19

    A.2 错误码说明 ..... 20

附录 B (规范性) 协议安全要求 ..... 21

    B.1 协议通道安全要求 ..... 21



B.2 重定向端点安全要求 ..... 21

B.3 客户端身份鉴别安全要求 ..... 21

B.4 授权码流程中的安全要求 ..... 22

B.5 客户端身份凭据许可流程中的安全要求 ..... 22

B.6 设备授权许可机制中的安全要求 ..... 22

B.7 访问令牌安全要求 ..... 22

B.8 刷新令牌安全要求 ..... 23

参考文献 ..... 24



# 前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国网络安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国科学院信息工程研究所、北京数字认证股份有限公司、国民认证科技(重庆)有限公司、大唐高鸿信安(浙江)信息科技有限公司、中国科学院软件研究所、中国信息通信研究院、湖北省数字证书认证管理中心有限公司、北京银联金卡科技有限公司、北京快手科技有限公司、联通在线信息科技有限公司、中电信量子信息科技集团有限公司、长扬科技(北京)股份有限公司、高颂数科(厦门)智能技术有限公司、浙江大华技术股份有限公司、中金金融认证中心有限公司、奇安信网神技术(北京)股份有限公司。

本文件主要起草人：高能、李敏、张靖炜、刘丽敏、刘海洁、查达仁、彭佳、屠晨阳、杨昀、夏琦清、李业旺、曾亮、张亚男、李俊、张立武、穆域博、柴瑶琳、陈诚、陈跃、刘冠廷、程福兴、刘勇、赵华、范中益、李超、刘红日、安锦程。



## 引 言

本文件规定的协议实现了资源所有者在不共享凭据(如用户名和口令)的情况下,将资源所有者在资源服务器的资源,以安全、可控的方式开放给外部接入的客户端使用,实现资源访问能力的开放与可控共享。

本文件参考国际互联网工程任务组(The Internet Engineering Task Force,简称 IETF)的 RFC 6749、OAuth 2.1 等主流授权协议和最佳实践,并结合我国相关密码算法和产业现状进行制定。本文件与国际 OAuth 协议是兼容扩展关系,按我国相关密码政策和法规,结合我国实际应用需求及产品生产厂商的实践经验,本文件在客户端身份鉴别部分增加了基于 SM2 的数字证书鉴别方法。通信安全优先采用 GB/T 38636 规定的 TLCP,因国际互通场景或因系统兼容导致不能使用 TLCP 时,可使用 TLS 协议,并优先选用国密算法套件的 TLS 连接。对访问令牌的保护增加了采用 SM2、SM3、SM4 等算法对其进行签名和加密的规定。



# 网络安全技术

## 开放的第三方资源授权协议

### 1 范围

本文件确立了开放的第三方资源授权协议的通则,规定了客户端类型和要求,以及不同类型的授权流程、令牌发放与刷新、受保护资源访问的协议要求。

本文件适用于跨安全域应用场景下,基于 HTTP 通信机制的资源授权服务的设计与开发。

### 2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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 信息安全技术 SM3 密码杂凑算法
- GB/T 32907 信息安全技术 SM4 分组密码算法
- GB/T 32918.2 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 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
- GB/T 38636 信息安全技术 传输层密码协议(TLCP)

### 3 术语和定义

下列术语和定义适用于本文件。

#### 3.1

**授权 authorization**  
授予访问者访问受保护资源的权限。

#### 3.2

**资源所有者 resource owner**  
对受保护资源享有所有权,并有权决定受保护资源访问权限的实体。  
注:资源所有者可以是自然人,也可以是代表组织或系统的其他实体,当资源所有者是自然人时,称为终端用户。

#### 3.3

**资源服务器 resource server**  
存储受保护资源,并能接收和响应受保护资源访问请求的服务器。

#### 3.4

**客户端 client**  
代表资源所有者请求访问受保护资源的应用程序。

#### 3.5

**第三方应用 third party application**  
相对于资源所有者及资源服务器所属域而言的外部应用或服务,获得资源所有者授权后代表其访问受保护资源。

注：第三方在获得资源所有者授权后代表其访问受保护资源体，本文件中简称“第三方”，功能角色为客户端。

3.6

**授权服务器 authorization server**

对客户端进行授权的服务器。

注：授权服务器与资源服务器可是同一实体，也可是相互分离的 2 个实体。同一台授权服务器所发放的访问令牌可被多台资源服务器识别和接受。

3.7

**端点 endpoint**

用于接收请求消息、返回响应消息的接口。

3.8

**重定向端点 redirection endpoint**

客户端上用于接收授权响应的端点。

3.9

**授权端点 authorization endpoint**

授权服务器上用于与资源所有者交互的端点。

注：用于接收客户端的授权请求、获取资源所有者的授权决定，并在授权完成后向客户端返回授权结果。

3.10

**令牌端点 token endpoint**

授权服务器上用于与客户端交互的端点。

注：授权服务器使用该端点接收客户端发起的令牌请求，当授权服务器验证请求成功后，通过该端点返回令牌给客户端。

3.11

**授权码 authorization code**

授权服务器发放给客户端的、能表明资源所有者同意客户端访问受保护资源的凭据。

注：客户端使用授权码获取访问令牌和刷新令牌。

3.12

**授权许可 authorization grant**

代表资源所有者同意客户端访问其受保护资源的授权凭据。

注：本文件定义的授权许可类型包括授权码许可、客户端身份凭据许可、设备授权许可。客户端凭此凭据向授权服务器换取访问令牌，不直接用于访问受保护资源。

3.13

**验证码 code\_verifier**

客户端为每个授权请求生成的随机字符串。

3.14

**令牌 token**

授权服务器发放给客户端的凭据。

注：令牌分为访问令牌和刷新令牌 2 种类型。

3.15

**访问令牌 access token**

授权服务器颁发给客户端的、用于访问特定范围内受保护资源的授权凭据。

3.16

**刷新令牌 refresh token**

授权服务器颁发给客户端的、用于在无需资源所有者再次参与的情况下获取新访问令牌的凭据。

注：当访问令牌过期、失效或需要缩小权限范围时，客户端使用此凭据向授权服务器换取新访问令牌。



4 缩略语

下列缩略语适用于本文件。  
HTML:超文本置标语言(Hypertext Markup Language)  
HTTP:超文本传输协议(Hypertext Transfer Protocol)  
TLCP:传输层密码协议(Transport Layer Cryptographic Protocol)  
TLS:安全传输层(Transport Layer Security)  
UTF-8:UCS 变换形式 8(UCS Transformation Format 8)  
URI:统一资源标识符(Uniform Resource Identifier)  
URL:统一资源定位符(Uniform Resource Locator)

5 通则

5.1 协议角色

协议角色如下。

- 资源所有者:负责决策是否授予受保护资源的访问权限,并在鉴别过程中提供身份凭证。
- 服务提供者:资源服务器或授权服务器所属平台或服务。授权服务器负责对资源所有者进行身份鉴别,验证客户端合法性和真实性,并根据资源所有者的授权意愿确定是否颁发授权许、访问令牌。资源服务器负责托管受保护资源,接收并校验客户端提交的访问令牌,根据校验结果响应资源请求。
- 客户端(第三方应用):负责向资源拥有者发起授权请求,并代表资源拥有者使用令牌访问受保护资源。

5.2 协议基本流程

协议基本流程见图 1,图 1 给出了资源所有者、服务提供者和客户端等三个角色之间的关系。

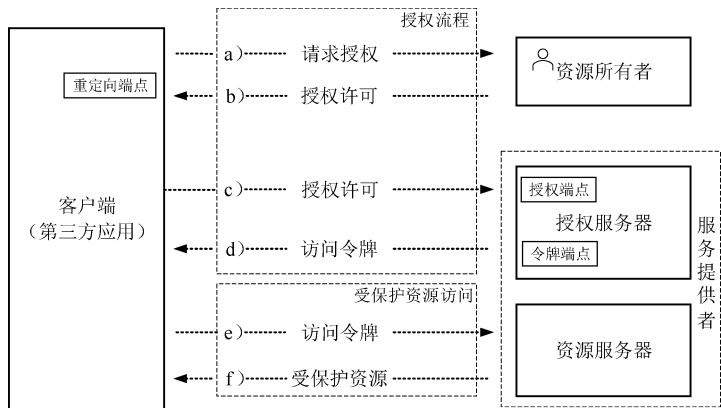


图 1 协议基本流程

图 1 包括以下步骤。

- a) 客户端向资源所有者请求授权。客户端不直接与资源所有者交互,而是通过授权服务器作为中介发送请求给资源所有者[见 7.2.1 的 a)、b)]。
- b) 资源所有者确认授权后,授权服务器依据该授权意愿向客户端发放授权许可。

- c) 客户端向授权服务器提交授权许可以及身份凭据,向授权服务器请求访问令牌。
- d) 授权服务器鉴别客户端的身份并验证授权许可的有效性,如客户端身份鉴别通过且授权许可有效,则授权服务器向客户端发放访问令牌。
- e) 客户端向资源服务器发送访问令牌及相关参数,用以请求访问受保护资源。
- f) 资源服务器验证访问令牌的有效性。如访问令牌有效,则将请求的资源发送给客户端,如客户端对受保护资源的访问超出访问令牌范围或有效期,则访问失效,客户端重新开始授权请求或采用 8.3 的规定进行访问令牌刷新。

协议基本流程主要包括授权流程和受保护资源访问两个阶段。具体授权流程见第 7 章,资源访问见第 9 章。

本文件规定的授权协议构建于 HTTP 之上。协议参数说明见附录 A。协议通道安全要求应符合 B.1。

### 5.3 协议端点类型

#### 5.3.1 端点分类

本文件规定了三种功能的端点:

- a) 授权端点;
- b) 令牌端点;
- c) 重定向端点。

授权端点和令牌端点允许客户端在请求中添加能表明访问范围的参数,用该参数指明资源访问请求中请求的受保护资源访问范围。相应地,授权服务器通过在响应中包含访问范围的参数来告知客户端其被发放的访问令牌的受保护资源访问范围。若实际授予的访问范围与请求的不一致,响应中给出表示实际访问范围的参数,以告知客户端其实际被允许的受保护资源访问范围。

如客户端在请求授权时省略了范围参数,授权服务器使用预定义的默认值回应此请求,或者拒绝此次请求。授权服务器在其服务文档中对范围参数的要求和默认值进行说明。

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)]。其中查询组件和片段组件采用“application/x-www-form-urlencoded”编码格式。

**示例:** 在 `https://example.com/authorize? response_type = code&client_id = s6BhdRkqt3 # section1` 中,方案为 `https`,主机名为 `example.com`,路径为 `/authorize`,查询组件为 `response_type = code&client_id = s6BhdRkqt3`,片段组件为 `section1`。

#### 5.3.2 授权端点

授权端点位于授权服务器,接收客户端的授权请求、资源所有者的身份凭据和授权,并通过用户代理重定向到客户端重定向端点并附带授权码。当授权服务器收到客户端的授权请求时,授权服务器首先验证资源所有者的身份。

授权端点 URI 通常由授权服务器的服务文档提供。

授权端点的 URI 可包含查询组件。当增加其他查询参数时,保留该查询组件,该端点 URI 不包含片段组件。

授权服务器的授权端点应具备处理 HTTP GET 请求的能力,可具备处理 HTTP POST 请求的能力。

#### 5.3.3 令牌端点

客户端呈递授权许可或刷新令牌给授权服务器的令牌端点,授权服务器验证请求后,令牌端点发放

访问令牌给客户端。

本文件不规定客户端获取令牌端点 URI 的方式(通常由授权服务器的服务文档提供)。

令牌端点 URI 可包含查询组件。当增加其他查询参数时,保留该查询组件。令牌端点 URI 不包含片段组件。

客户端在向授权服务器的令牌端点请求访问令牌时使用 HTTP POST 方法。

当授权服务器的令牌端点收到具备凭据保护能力的客户端或其他被授予了身份凭据的客户端的请求时,授权服务器对客户端进行身份鉴别。

#### 5.3.4 重定向端点

客户端在其注册阶段预先向授权服务器注册 URI 作为重定向端点。授权服务器完成与资源所有者的交互之后,将资源所有者的用户代理重定向到客户端的重定向端点,向客户端返回授权结果。

重定向端点 URI 是绝对 URI。重定向端点 URI 可包含查询组件,在向重定向端点 URI 添加其他查询参数时,保留该组件。重定向端点 URI 不包含片段组件。

重定向端点安全要求应符合 B.2。



## 6 客户端类型和要求

### 6.1 类型

根据客户端是否对其身份凭据具有保护能力,本文件规定了两种客户端的类型:

#### a) 具备凭据保护能力的客户端

客户端有能力维持其凭据的机密性(例如,客户端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,或者客户端有能力通过其他方式(超出本文件的范围)证明自己身份的真实性;

注:典型代表为 Web 应用,资源所有者通过 HTML 用户界面来访问该应用,此 HTML 用户界面由其使用的设备中的用户代理来渲染。客户端身份凭据以及发放给客户端的所有访问令牌都存储在 Web 服务器上,对资源所有者而言是不可获取且不可访问的。

#### b) 不具备凭据保护能力的客户端

客户端没有能力维持其凭据的机密性(例如,客户端运行在资源所有者使用的设备上,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,并没有能力通过其他方式证明自己身份的真实性。

注:典型代表为运行于用户代理上的应用和本地应用。运行于用户代理的应用从 Web 服务器下载到资源所有者本地设备上并在用户代理(如 Web 浏览器)中执行,其协议数据和凭据对于资源所有者可访问。本地应用安装并运行在资源所有者所使用的设备上,其协议数据和凭据对资源所有者是可访问的。

客户端类型的认定取决于授权服务器的鉴别安全需求和授权服务器对客户端身份凭据被获取风险的接受程度(通常由授权服务器的服务文档提供)。授权服务器不对客户端的类型进行假定。

客户端可由一组分布式的组件共同实现,每个组件具有不同的客户端类型和安全上下文(例如,客户端同时具有基于服务器的具备凭据保护能力的组件和基于浏览器的不具备凭据保护能力的组件)。此类客户端的注册不在本文件中规定,通常客户端运营商可将客户端的每个组件都注册在授权服务器上。

### 6.2 标识符

客户端标识符是授权服务器为注册的客户端发放的应用程序标识符。该标识符是字符串,授权服务器使用该字符串可唯一标识一个客户端。

本文件对客户端标识符的长度不作规定。授权服务器宜在其服务文档中说明所发放客户端标识符的长度。

### 6.3 注册

在协议进行之前,客户端的提供商需要在授权服务器上注册客户端的信息(例如重定向端点 URI、客户端类型等),建立客户端与授权服务器的信任关系。客户端提供商使用授权服务器允许的注册方法(通常由授权服务器的服务文档提供)完成注册。

在注册客户端时,客户端提供商应提供以下信息给授权服务器:

- a) 客户端的类型;
- b) 指向客户端的重定向端点;
- c) 授权服务器所需要的其他信息(如,应用名称、网站和描述、客户端身份鉴别方法等)。

### 6.4 身份鉴别

#### 6.4.1 身份凭据鉴别方案

针对具备凭据保护能力的客户端,当授权服务器使用基于身份凭据的鉴别方案对客户端进行鉴别时,授权服务器应允许客户端在请求体中添加相关参数传递客户端身份凭据以进行身份鉴别,可允许客户端使用 HTTP 基本鉴别方案(见 RFC 9110)。当采用请求体中添加客户端身份凭据的身份鉴别方案时,应通过 POST 方式将如下参数放在 HTTP 主体部分进行传输,不应通过 HTTP GET 方式将参数包含在请求的 URI 中。

- a) client\_id [必选]

6.2 中所描述的客户端标识符。

- b) client\_secret [必选]

客户端密钥。

注 1: 该参数为授权服务器与客户端预先共享的对称密钥。

注 2: 当客户端注册阶段明确采用基于国产密码算法的身份凭据鉴别方案时,该参数值默认为基于 SM3 密码杂凑算法的消息鉴别码。以客户端密钥为键,以客户端标识符、生成的随机字符串和时间戳计算生成,生成方法见 GB/T 15852.2。

注 3: 因国际互通需求或系统兼容性导致不能使用国产密码算法时,该参数值可为客户端密钥的原文。

- c) nonce [条件必选]

客户端生成的随机字符串。当 client\_secret 采用注 2 所述的方法时,该参数为必选。

- d) timestamp [必选]

时间戳,当 client\_secret 采用注 2 所述的方法时,该参数为必选。

由于鉴别具备凭据保护能力的客户端的方法涉及客户端密钥,授权服务器应采取措施使所有涉及客户端密钥的端点具备抵御暴力攻击的能力。客户端身份鉴别安全要求应符合 B.3。

#### 6.4.2 数字证书鉴别方案

本文件推荐采用数字证书鉴别方案实现对客户端的身份鉴别。对于支持国产密码算法的客户端,在客户端注册阶段若明确采用数字证书鉴别方案,应使用符合 GB/T 32918.2 的 SM2 数字证书鉴别方案对客户端进行鉴别,宜采用 GB/T 15843.3 中的双向鉴别相关鉴别方案。客户端身份鉴别安全要求应符合 B.3。

#### 6.4.3 其他鉴别方案

授权服务器可采用任何符合其安全需求的鉴别方案。当采用其他鉴别方案时,授权服务器应记录

客户端标识符所对应的鉴别方案。

7 授权流程

7.1 授权许可类型

7.1.1 概述

本文件规定了三种授权许可类型：

- a) 授权码许可；
- b) 客户端身份凭据许可；
- c) 设备授权许可。

7.1.2 授权码许可

客户端不直接向资源所有者请求授权，而是以授权服务器为中介向资源所有者请求授权。客户端将资源所有者的用户代理重定向到授权服务器，授权服务器与资源所有者交互，对资源所有者的身份进行鉴别，并征得资源所有者授权后，将资源所有者的用户代理重定向回到客户端，并在重定向消息中携带授权码。

授权码许可流程适用于需要资源所有者参与授权，由客户端代表资源所有者访问受保护资源的通用场景。对于不具备凭据保护能力的客户端应使用授权码许可流程，对于具备凭据保护能力的客户端宜使用授权码许可流程。授权码许可类型可用于获取访问令牌和刷新令牌。

7.1.3 客户端身份凭据许可

客户端身份凭据(或其他形式的能用于客户端身份鉴别的信息)可作为授权许可，用于获取访问令牌。客户端身份凭据许可是一种受限场景下进行授权的方法。客户端身份凭据许可类型适用于以下受限场景：

- a) 受保护资源由客户端控制的场景；
- b) 经协商，授权服务器同意客户端访问受保护资源的场景。

7.1.4 设备授权许可

设备授权许可是一种用于在输入受限设备(例如智能电视、打印机等)上进行授权的方法。设备授权许可允许用户通过具备标准网页浏览器的设备(如智能移动通信终端)来完成授权。

7.2 授权码许可

7.2.1 流程

授权码许可流程见图 2。



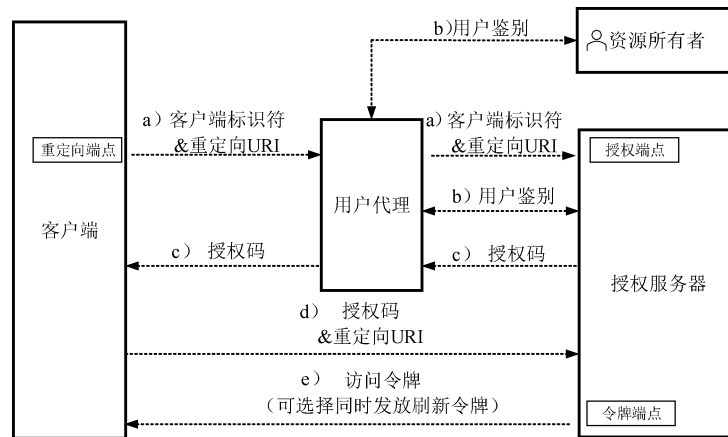


图 2 授权码许可流程

图 2 中包括以下步骤。

- 客户端构造通过将资源所有者的用户代理重定向到授权端点[图 2 中有 2 个 a)，即表示重定向的过程]，使用户代理自动向授权服务器发送 7.2.2 规定的授权请求。授权请求中包含客户端标识符、由验证码派生的挑战码、申请的受保护资源访问范围、本地状态和客户端的重定向端点 URI(图 2 中仅标出了客户端标识符和重定向端点 URI 作为示例，通常请求中会包括更多参数)，其中重定向端点 URI 用于客户端接收来自授权服务器的关于授权的结果。
- 授权服务器(通过用户代理)鉴别资源所有者并询问资源所有者是否允许客户端的访问请求[图 2 中的 2 个 b)表示授权服务器通过资源所有者的用户代理鉴别资源所有者的过程]。
- 如资源所有者同意了此次访问，授权服务器使用重定向端点 URI 将用户代理重定向到客户端[图 2 中有 2 个 c)，即表示重定向的过程]。重定向端点 URI 中包含授权码和步骤 a)中由客户端提供的本地状态(图 2 中未表示出本地状态)。
- 客户端向授权服务器的令牌端点发送访问 7.2.4 规定的令牌请求，该请求包含上一步骤中获得的授权码和验证码。在构造本次请求时，若客户端具备凭据保护能力，则向授权服务器提供身份凭据以便授权服务器对其进行身份鉴别。若客户端在授权请求中包含了重定向端点 URI，则在本次令牌请求中也应包含相同的重定向端点 URI。
- 授权服务器鉴别客户端，验证授权码的有效性，验证使用授权码的客户端与步骤 a)中请求授权的客户端的一致性，并核对收到的重定向端点 URI 与此前步骤 c)中的重定向端点 URI 的一致性。如验证通过，授权服务器返回访问令牌(可同时返回刷新令牌)给客户端。

授权码流程中的安全要求应符合 B.4。

### 7.2.2 授权请求

客户端通过将以下参数添加到授权端点 URI 的查询组件，来构造授权请求。

- response\_type [必选]  
参数值为“code”。
- client\_id [必选]  
6.2 中所描述的客户端标识符。
- code\_challenge [条件必选]  
挑战码，客户端生成的验证码 code\_verifier 的杂凑值，用于防止授权码被拦截和滥用，长度范围为 43~128 个字符，挑战码熵值不低于 256 位。挑战码生成方式优先采用国产密码算法 SM3 算法。仅当客户端为具备凭据保护能力的客户端，且采取等效安全机制防范授权码注入



或重放攻击时,可不包含该参数,其他情形均应包含该参数。

注:挑战码可通过三种方式生成,一是采用国产密码算法 SM3 算法进行杂凑和 BASE64URL 编码,二是对 code\_verifier 进行 SHA-256 杂凑运算后执行 BASE64URL 编码,三是直接使用原始 code\_verifier。第三种方式为明文模式,不宜使用。

d) code\_challenge\_method [可选]

生成挑战码的杂凑算法。如请求中未提供,则默认使用 SM3 算法,若因兼容性要求导致默认算法无法使用,则使用 SHA-256 算法,若无法使用该算法,则直接使用验证码 code\_verifier 作为挑战码 code\_challenge。

e) redirect\_uri [条件必选]

重定向 URI。如客户端仅注册了一个重定向 URI,则该参数为可选。如注册了多个重定向 URI,则该参数为必选。

f) scope [可选]

请求访问受保护资源的范围。以一组由空格间隔的大小写敏感的字符串表示。如参数值包含多个空格间隔的字符串,字符串的顺序不影响解析。参数值的具体含义由授权服务器规定,通常在其服务文档中予以说明。

g) state [可选]

7.2.1 步骤 a) 中的本地状态。该值应具备不可猜测性。授权服务器在将用户代理重定向回客户端时,在重定向请求中包含此值。客户端开发者宜使用该参数,以防止跨站点请求伪造攻击。

授权服务器验证授权请求的有效性,检查所有必选参数都存在且有效。如验证请求有效,授权服务器应对资源所有者的身份进行鉴别并从资源所有者处获得授权决定(通过直接询问资源所有者的方式或其他方式)。

## 7.2.3 授权响应

### 7.2.3.1 正确响应

如资源所有者允许本次授权请求,授权服务器通过重定向的方式给客户端发放授权码,并将该授权码与接收到的客户端授权请求中的 code\_challenge(挑战码)关联存储。授权服务器向重定向端点 URI 的查询组件添加如下参数。

a) code [必选]

由授权服务器产生的授权码。为降低泄露的风险,该授权码在发放后短时间内失效。推荐授权码最长生存周期为 10 min。客户端不得重复使用该授权码。如授权码被重复使用,授权服务器拒绝该次请求并撤销此前基于该授权码所发放的所有访问令牌。授权服务器将授权码与客户端标识符、重定向 URI 进行绑定。

b) state [条件必选]

如客户端的授权请求中含有此参数,则授权响应中也包含此参数。该参数的值与客户端授权请求中的 state 值相同。

参数采用 UTF-8 进行 URL 编码。在 Web 浏览器环境下,参数通常以 application/x-www-form-urlencoded 格式附加于重定向 URI 的查询组件;在移动应用等特定环境下,应根据其采用的重定向机制实现编码的兼容性。

客户端忽略未识别的响应参数。本文件对授权码的字符串长度不做规定。客户端不宜对字符串长度做出规定。授权服务器在服务文档中说明其发放所有参数值的长度。

### 7.2.3.2 出错响应

如由于重定向端点 URI 丢失、无效或不匹配,或由于客户端标识符丢失或无效等原因出错,授权服务器应告知资源所有者这一错误,并且不应自动将用户代理重定向至无效的重定向端点 URI。

如由于资源所有者拒绝访问请求或是由于重定向端点 URI 有误之外的其他原因导致授权失败,授权服务器向重定向端点 URI 的查询组件添加如下参数,以通知客户端出错原因。

a) error [必选]

错误代码,错误代码类型如下所示:

- 1) invalid\_request 表示请求中丢失了必选参数,或存在无效参数,或重复包含了某个参数,或是其他形式的格式错误;
- 2) unauthorized\_client 表示该客户端无权使用当前方法请求授权码;
- 3) access\_denied 表示授权服务器拒绝访问请求(注:不区分资源所有者拒绝请求和授权服务器拒绝请求,均采用相同的错误代码类型);
- 4) unsupported\_response\_type 表示授权服务器不接受使用该方法获取授权码;
- 5) invalid\_scope 表示所请求的资源访问范围无效、未知或是形式不当;
- 6) server\_error 表示授权服务器遇到了意外情况从而无法响应该请求(该错误代码是需要的,因为 HTTP 的 500 内部服务器错误代码无法通过 HTTP 重定向返回);
- 7) temporarily\_unavailable 表示由于暂时的过载或是服务器维护,授权服务器目前无法处理该请求(该错误代码是需要的,因为 HTTP 的 503 服务错误代码无法通过 HTTP 重定向返回)。

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

b) error\_description [可选]

终端用户可读的文本,提供附加信息以帮助客户端的开发者理解出现的错误。该参数的值不包含 %x20-21/%x23-5B/%x5D-7E 集合之外的字符。

c) error\_uri [可选]

用于标识网页,该网页含有终端用户可读的、关于该错误更多信息。该参数的值符合 URI-reference 语法,并且不得包含 %x20-21/%x23-5B/%x5D-7E 集合之外的字符。

d) state [条件必选]

如客户端的授权请求中含有此参数,则响应中也应包含此参数。响应中该参数的值与授权请求中的值相同。

## 7.2.4 访问令牌请求

### 7.2.4.1 令牌请求参数

客户端向令牌端点发送请求,以获取访问令牌。客户端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]

参数值为“authorization\_code”。

b) code[必选]

从授权服务器获得的授权码。

c) code\_verifier[条件必选]

验证码,即客户端为每个授权请求生成的随机字符串。当且仅当授权请求中包含 code\_challenge 参数时为必选。验证码是为每个授权请求生成的唯一的高熵(熵值不低于 256 位)随机



字符串,使用非保留字符[a-z]/[a-z]/[0-9]/“-”/“.”/“\_”/“~”,最小长度 43 个字符,最大长度 128 个字符。

- d) redirect\_uri[条件必选]  
如客户端在授权请求中包含此参数,则在该请求中也包含此参数,且二次的参数值应保持一致。
- e) client\_id[条件必选]  
客户端标识符,如客户端未按 6.4 所述方式被授权服务器鉴别身份,则客户端在该请求中添加此参数。
- f) client\_secret[可选]  
客户端的口令。如客户端的类型为具备凭据保护能力,可使用该参数实现授权服务器对该客户端的身份鉴别。

#### 7.2.4.2 令牌请求处理要求

授权码许可流程中,授权服务器应满足如下要求。

- 对具备凭据保护能力的客户端或已被发放过客户端身份凭据(或被其他鉴别要求所约束)的客户端进行身份鉴别。
- 将授权码发放给正确客户端。对具备凭据保护能力的客户端,通过客户端身份鉴别确认其身份,对不具备凭据保护能力的客户端,以请求中的 `client_id` 标识其身份。
- 验证授权码是否有效,包括是否在有效期内,是否未被使用,以及是否与 `redirect_uri` 绑定关系一致等。
- 当授权请求包含验证码时,令牌请求应包含 `code_verifier` 参数。当授权请求未包含验证码时,令牌请求不应包含验证码。
- 当授权请求包含验证码时,应对验证码校验,采用与授权请求相同的杂凑算法对验证码进行运算,且将运算结果与预存的挑战码对比,若不一致则拒绝令牌请求。
- 除客户端具备凭据保护能力且采取等效安全机制防范授权码注入或重放攻击的情形外,若与该授权码关联的授权请求中未包含验证码,授权服务器应拒绝该令牌请求。
- 若授权请求中包含 `redirect_uri` 参数,则令牌请求中也应包含该参数,且两次提供的参数值应一致。

### 7.2.5 访问令牌响应

如访问令牌请求是有效的,授权服务器按第 8 章所述发放访问令牌和刷新令牌(可选)。如授权服务器对发起访问令牌请求的客户端的身份鉴别失败,或对访问令牌请求的验证失败,授权服务器返回 8.2.3 所述的出错响应。

### 7.3 客户端身份凭据许可

### 7.3.1 流程

客户端身份凭据许可流程见图 3。

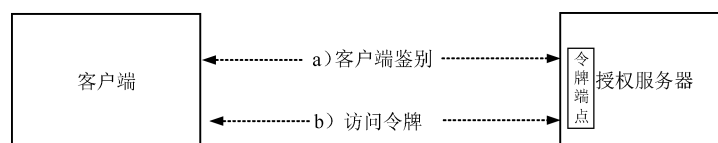


图 3 客户端身份凭据许可流程

图 3 包括以下步骤：

- a) 客户端向授权服务器的令牌端点发送访问令牌请求，并提交客户端身份凭据，授权服务器对客户端进行身份鉴别；
  - b) 授权服务器鉴别客户端的身份，如身份鉴别通过，则发放访问令牌。
- 客户端身份凭据许可流程中的安全要求应符合 B.5。

7.3.2 授权请求和响应

客户端鉴别结果被用作授权许可，无需额外的授权请求。

7.3.3 访问令牌请求

客户端向令牌端点发送请求，在该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]  
参数值为“client\_credentials”；
- b) client\_id [必选]  
6.2 中所描述的客户端标识符；
- c) scope [可选]  
请求访问受保护资源的范围。

授权服务器根据 6.4 给出的身份鉴别方法对客户端进行身份鉴别。

7.3.4 访问令牌响应

如访问令牌请求是有效的，授权服务器按 8.2.1 所述发放访问令牌，响应中不应包含刷新令牌。如授权服务器对发起访问令牌请求的客户端的身份鉴别失败，或对客户端请求的验证失败，则授权服务器返回 8.2.3 所述的出错响应。

7.4 设备授权许可

7.4.1 流程

设备授权许可流程见图 4。

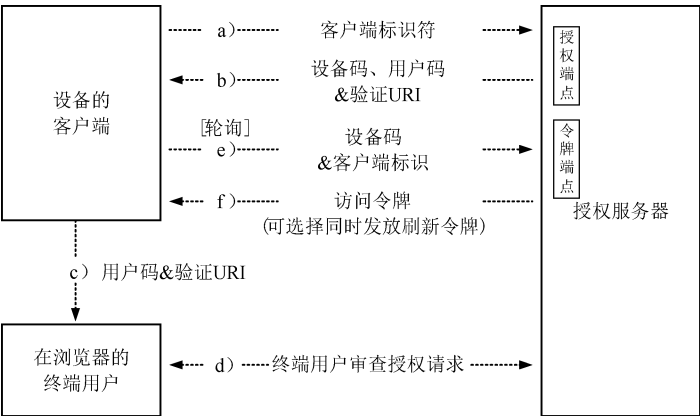


图 4 设备授权许可流程

图 4 包括以下步骤。

- a) 设备的客户端向授权服务器请求访问权限，并在请求中包含客户端标识符。

- b) 授权服务器向设备的客户端颁发设备码、用户码和用户验证 URI。
- c) 设备的客户端指示用户在另一台设备上使用用户代理访问提供的用户验证 URI,并向用户提供终端用户码。
- d) 授权服务器通过用户代理对终端用户进行身份鉴别,并提示用户输入设备的客户端提供的用户码。授权服务器验证用户提供的用户码,并提示用户接受或拒绝请求。
- e) 在终端用户审核客户端授权请求[步骤 d)]期间,客户端反复轮询授权服务器,以了解用户是否完成了用户授权步骤。轮询请求中包含设备代码及其客户端标识符。
- f) 授权服务器验证设备的客户端提供的设备码,并在设备的客户端被授予访问权限时响应访问令牌,如被拒绝访问则返回错误,或者指示设备的客户端继续轮询。

设备授权许可机制中的安全要求应符合 B.6。

## 7.4.2 授权请求


客户端向设备授权服务器发出 HTTP“POST”请求,请求中包含如下参数:

- a) client\_id [必选]  
6.2 中所描述的客户端标识符;
- b) scope [可选]  
请求访问受保护资源的范围。

## 7.4.3 授权响应

### 7.4.3.1 正确响应

授权服务器生成唯一的设备码和用户码,并添加到 HTTP 响应主体中,响应参数如下:

- a) device\_code [必选]  
设备码; 
- b) user\_code [必选]  
用户码;
- c) verification\_uri [必选]  
验证 URI;
- d) verification\_uri\_complete [可选]  
包含用户码(或与用户码有相同功能的其他信息)的验证 URI,用于非文本传输;
- e) expires\_in [必选]  
设备码和用户码的有效期,以秒为单位;
- f) interval [可选]  
客户端在向令牌端点轮询请求之间应该等待的最小时间,如响应中不包含该参数,默认值为 5 s。

### 7.4.3.2 出错响应

如出现错误,则授权服务器发送出错响应,以通知客户端出错原因。

- a) error [必选]  
错误代码,错误代码类型如下:
  - 1) invalid\_request 表示请求中丢失了必选参数,或存在无效参数,或重复包含了某个参数,或是其他形式的格式错误;
  - 2) invalid\_client 表示客户端身份鉴别失败;

- 3) `invalid_grant` 表示所提供的授权许可无效、已过期、已撤销、不匹配重定向端点 URI, 或该授权许可并非颁发给当前客户端;
- 4) `unauthorized_client` 表示该客户端无权使用当前方法请求授权码;
- 5) `unsupported_grant_type` 表示该客户端未被授权使用当前授权许可类型;
- 6) `invalid_scope` 表示所请求的资源访问范围无效、未知或是形式不当。  
`error` 参数的值不包含 `%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 ASCII 文本, 提供附加信息以帮助客户端的开发者理解出现的错误。该参数的值不包含 `%x20-21/%x23-5B/%x5D-7E` 集合之外的字符。
- c) `error_uri` [可选]  
用于标识网页, 该网页含有终端用户可读的、关于该错误更多信息。该参数的值符合 URI-reference 语法, 并且不应包含 `%x20-21/%x23-5B/%x5D-7E` 集合之外的字符。

#### 7.4.4 访问令牌请求

客户端向令牌端点发送请求, 以获取访问令牌。客户端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]  
参数值为“urn:ietf:params:oauth:grant-type:device\_code”;
- b) `device_code` [必选]  
设备授权响应中的设备码;
- c) `client_id` [条件必选]  
客户端标识符, 如客户端未按 6.4 所述方式被授权服务器鉴别身份, 则客户端在该请求中添加此参数。

#### 7.4.5 访问令牌响应



如访问令牌请求是有效的, 授权服务器按 8.2.1 所述发放访问令牌和刷新令牌(可选的)。如授权服务器对发起访问令牌请求的客户端的身份鉴别失败, 或对访问令牌请求的验证失败, 授权服务器返回 8.2.3 所述的出错响应。除了 8.2.3 所述的错误代码外, 还有如下错误代码:

- a) `authorization_pending` 表示授权请求仍在等待中, 因为用户尚未完成用户交互步骤;
- b) `slow_down` 是“authorization\_pending”的一种变体, 授权请求仍在等待中并且轮询继续;
- c) `access_denied` 表示授权请求被拒绝;
- d) `expired_token` 表示“device\_code”已过期, 设备授权会话已结束。客户端可开始新的设备授权请求, 但需等待用户交互后再重新启动, 以避免不必要的轮询。

### 8 令牌发放与刷新

#### 8.1 令牌类型

##### 8.1.1 访问令牌

访问令牌是授权服务器发放给客户端用于访问受保护资源的凭据。访问令牌使用字符串表示, 表明客户端拥有了资源所有者的授权。访问令牌对于客户端而言通常是不易解读的。访问令牌中给出了受保护资源的访问范围和访问有效期, 访问范围和访问有效期由资源所有者授权同意, 并由资源服务器和授权服务器实施。

访问令牌可作为提取授权信息的标识符,也可包含授权信息,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,包含数据和签名)。本文件中建议授权服务器优先采用符合 GB/T 32905 的 SM3 算法对访问令牌的内容进行杂凑运算,再使用符合 GB/T 32918.2 的 SM2 算法或其他相关算法进行签名,最后使用符合 GB/T 32907 的 SM4 算法或其他相关算法对其加密,将最后签名加密处理过的令牌发送出去。访问令牌包含了客户端请求受保护资源所需的必要信息。

每种访问令牌类型应由相应的规范进行定义。若客户端无法识别某访问令牌类型,则不应使用该令牌。当访问令牌类型的定义中包含 8.2.2 规定之外的扩展参数时,应同时规定访问令牌的验证方法。

本文件不规定资源服务器验证访问令牌有效性的方法。访问令牌安全要求应符合 B.7。

### 8.1.2 刷新令牌

刷新令牌是客户端重新获取访问令牌的凭据。刷新令牌由授权服务器发放给客户端,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(访问令牌的生存周期和权限可小于资源所有者的授权范围)。如授权服务器决定发放刷新令牌给客户端,刷新令牌与访问令牌同时发放。

刷新令牌使用字符串表示,代表资源所有者的授权。刷新令牌的内部结构对客户端通常是不易解析的。刷新令牌是表示资源所有者授予客户端授权的字符串标识符,刷新令牌中不应包含授权信息。与访问令牌不同,刷新令牌只用于客户端与授权服务器的交互,不发送给资源服务器。

## 8.2 访问令牌发放

### 8.2.1 概述

如访问令牌请求是有效的,授权服务器按 8.2.2 所述发放访问令牌和刷新令牌(可选)。如授权服务器对发起访问令牌请求的客户端的身份鉴别失败,或对客户端的访问令牌请求验证失败,则授权服务器返回 8.2.3 所述的出错响应。

### 8.2.2 成功响应

授权服务器将如下参数添加到状态码是 200 的 HTTP 响应中,构造成功响应来发放访问令牌和刷新令牌(可选)。

- a) access\_token [必选]  
授权服务器发放的访问令牌。
- b) token\_type [必选]  
令牌类型。
- c) expires\_in [推荐]  
访问令牌的生存周期,以秒为单位。例如,“3600”表示该访问令牌将在响应发出 1 h 后过期。如本参数被省略,授权服务器当通过其他方式(例如公布缺省值)提供过期时间。
- d) refresh\_token [可选];  
刷新令牌。
- e) scope [条件必选]  
如该参数的值与客户端访问令牌请求中的 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。

对于任何包含令牌等敏感信息的响应,授权服务器在 HTTP 响应的头部中包含值为“no-store”的“Cache-Control”字段,以及值为“no-cache”的“Pragma”字段。

客户端忽略未识别的响应参数。本文件对授权码的字符串长度不做规定。客户端不宜对字符串长

度做出假定。授权服务器在服务文档中说明其发放的所有参数值的长度。

### 8.2.3 出错响应

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]

错误代码,有以下类型。

- 1) invalid\_request 表示该请求缺失了必选参数,或包含了不被接受的参数值,或重复包含了某一参数,或包含了多个凭据,或使用了超过一种的客户端身份鉴别的方式等。
- 2) invalid\_client 表示鉴别客户端身份失败(例如,客户端未知,或访问令牌请求中未包含 6.4 规定的客户端身份鉴别信息,或采用了不被接受的身份鉴别方式)。授权服务器可返回状态码为 401 的 HTTP 响应,用以表明可采用的 HTTP 鉴别方案。如客户端是通过请求头部的“Authorization”字段进行身份鉴别,但身份鉴别失败,授权服务器返回状态码为 401 的 HTTP 响应,并在头部中包含与客户端使用的鉴别方案匹配的“WWW-Authentication”头字段。
- 3) invalid\_grant 表示客户端提供的授权许可(例如,授权码)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,或是发放给另外的客户端的。
- 4) unauthorized\_client 表示授权服务器不允许该客户端使用当前授权许可类型。
- 5) unsupported\_grant\_type 授权服务器不接受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资源所有者授权的范围。

error 参数的值不包含 %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 ASCII 文本,提供附加信息以帮助客户端的开发者理解出现的错误,该参数的值不包含 %x20-21/%x23-5B/%x5D-7E 集合之外的字符。

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。该参数的值应符合 URI-reference 语法,并且不包含 %x20-21/%x23-5B/%x5D-7E 集合之外的字符。

## 8.3 访问令牌刷新

### 8.3.1 刷新流程

访问令牌刷新流程见图 5。





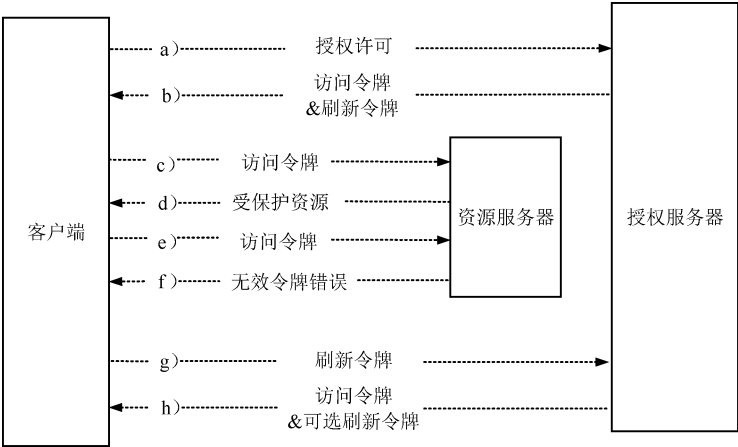


图 5 访问令牌刷新流程

图 5 包括以下步骤。

- a) 客户端鉴别授权服务器的身份并呈递授权许可，以此来请求访问令牌和刷新令牌。
- b) 授权服务器鉴别客户端的身份并验证授权许可的有效性。如身份鉴别通过且授权许可有效，则发放访问令牌和刷新令牌。
- c) 客户端向资源服务器呈递访问令牌，请求访问受保护资源。
- d) 资源服务器验证访问令牌的有效性。如访问令牌有效，则受理该请求。
- e) 重复执行步骤 c) 和 d)，直到访问令牌过期。在访问令牌过期的情况下，执行步骤 g)，否则继续请求访问受保护资源。
- f) 如访问令牌无效，资源服务器返回访问令牌无效的出错响应。
- g) 客户端鉴别授权服务器的身份并呈递刷新令牌，以此来请求新的访问令牌。授权服务器是否需要再次鉴别客户端的身份取决于客户端的类型和授权服务器的策略（通常由授权服务器的服务文档提供）。
- h) 授权服务器鉴别客户端的身份并验证刷新令牌的有效性，如刷新令牌有效，则向客户端发放新的访问令牌（或者同时发放新的刷新令牌[可选的]）。

本文件不对步骤 c)、d)、e)、f)的具体内容和实现进行规定。刷新令牌安全要求应符合 B.8。

8.3.2 请求和响应

如客户端接收到授权服务器发放的刷新令牌，则客户端可利用刷新令牌向令牌端点发送请求以获得新的访问令牌。客户端在访问令牌的刷新请求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]  
参数值为“refresh\_token”。
- b) client\_id [必选]  
6.2 中所描述的客户端标识符。
- c) refresh\_token [必选]  
授权服务器发放给客户端的刷新令牌。
- d) scope [可选]  
请求访问受保护资源的范围。请求中的受保护资源访问范围不应超出资源所有者最初许可的受保护资源访问范围，如该参数被省略，则缺省为资源所有者最初许可的受保护资源访问

范围。

授权服务器在发放刷新令牌时,将刷新令牌与被发放该刷新令牌的客户端绑定。在接收到访问令牌的刷新请求时,授权服务器应对具备凭据保护能力的客户端或已被发放过客户端身份凭据(或被其他鉴别要求所约束)的客户端进行身份鉴别。如需要鉴别该客户端,则执行鉴别流程,并确认刷新令牌发放给通过身份鉴别的客户端。授权服务器应对刷新令牌的有效性进行验证。

如访问令牌的刷新请求是有效的,授权服务器按 8.2 所述发放访问令牌。如对当前请求的客户端的身份鉴别失败或刷新令牌验证失败,授权服务器返回 8.2.3 所述的出错响应。

授权服务器可在发放新的访问令牌的同时发放新的刷新令牌,在此种情况下,客户端丢弃旧的刷新令牌,代之以新的刷新令牌。在向客户端发放了新的刷新令牌后,授权服务器可撤销旧的刷新令牌。如授权服务器发放了新的刷新令牌,新发放的刷新令牌的受保护资源访问范围与客户端在访问令牌的刷新请求中的受保护资源访问范围相同。

对于不具备凭据保护能力的客户端,刷新令牌应为一次性令牌或受到发送方约束的令牌,其中,约束条件可要求刷新令牌与客户端绑定。

## 9 受保护资源访问

### 9.1 受保护资源访问

客户端向资源服务器呈递访问令牌来访问受保护的资源。资源服务器验证访问令牌的有效性,包括验证访问令牌是否过期,以及访问令牌的受保护资源访问范围是否涵盖客户端请求访问的资源。

### 9.2 成功响应

当访问受保护资源的请求成功时,资源服务器告知客户端,并允许客户端访问受保护的资源。

### 9.3 出错响应

如访问受保护资源的请求失败,资源服务器应告知客户端这一错误。

开发者在设计令牌验证方案时,规定一种向客户端返回错误状态码的机制,规范协议参与方可理解的、达成一致的错误码及错误码值。令牌验证方案可将有效的错误值集合限定为本文件所列出的子集。如错误码通过参数返回,参数名为“error”。

其他现有的能用于本文件令牌验证的方案,可将其错误值与注册表中的值进行绑定。

令牌验证方案可选择 `error_description` 和 `error_uri` 参数来返回错误信息,但不与本文件中 `error_description` 和 `error_uri` 参数的使用互相冲突。



附 录 A  
(资料性)  
协议参数说明

### A.1 参数说明

本文件对协议参数进行说明,包括授权端点请求、授权端点响应、令牌端点请求或者令牌端点响应中的关键参数;

- a) 参数名称:client\_id  
参数使用的地方:授权请求,令牌请求;
- b) 参数名称:client\_secret  
参数使用的地方:令牌请求;
- c) 参数名称:response\_type  
参数使用的地方:授权请求;
- d) 参数名称:redirect\_uri  
参数使用的地方:授权请求,令牌请求;
- e) 参数名称:scope  
参数使用的地方:授权请求,授权响应,令牌请求,令牌响应;
- f) 参数名称:state  
参数使用的地方:授权请求,授权响应;
- g) 参数名称:code  
参数使用的地方:授权响应,令牌请求;
- h) 参数名称:error\_description  
参数使用的地方:授权响应,令牌响应;
- i) 参数名称:error\_uri  
参数使用的地方:授权响应,令牌响应;
- j) 参数名称:grant\_type  
参数使用的地方:令牌请求;
- k) 参数名称:access\_token  
参数使用的地方:令牌响应,资源访问请求;
- l) 参数名称:token\_type  
参数使用的地方:授权响应,令牌响应;
- m) 参数名称:expires\_in  
参数使用的地方:授权响应,令牌响应;
- n) 参数名称:refresh\_token  
参数使用的地方:令牌请求,令牌响应;
- o) 参数名称:token  
参数使用的地方:令牌请求,令牌响应;
- p) 参数名称:code\_verifier  
参数使用的地方:授权请求、令牌请求;
- q) 参数名称:code\_challenge  
参数使用的地方:授权请求;

- r) 参数名称:code\_challenge\_method  
参数使用的地方:授权请求;
- s) 参数名称:device\_code  
参数使用的地方:设备授权端点响应、令牌端点请求;
- t) 参数名称:user\_code  
参数使用的地方:设备授权端点响应;
- u) 参数名称:verification\_uri  
参数使用的地方:授权响应;
- v) 参数名称:verification\_uri\_complete  
参数使用的地方:设备授权端点响应;
- w) 参数名称:interval  
参数使用的地方:授权响应。

## A.2 错误码说明

错误码包含错误码名称和错误码值,协议需统一规范一致的错误码。

错误码名称:所请求的名称(如 example)。错误码值由字符集中的%x20-21/%x23-5B/%x5D-7E组成。

错误码的使用场景:授权码许可出错响应(见 7.2.3.2),访问令牌发放出错响应(见 8.2.3)和受保护资源访问出错响应(见 9.3)。

相关协议扩展:与错误码一同使用的扩展许可类型、访问令牌类型或扩展参数的名称。



## 附 录 B

### (规范性)

### 协议安全要求

#### B.1 协议通道安全要求

对于授权码、访问令牌、刷新令牌以及客户端身份凭据等敏感的数据,不应采用明文传输方式,应采用 GB/T 38636 规定的 TLCP 传输。在国际互通场景或由于系统兼容性导致不能使用 TLCP 时,可使用 TLS 协议,并优先选用采用国密算法套件的 TLS 协议连接。授权服务器应与客户端进行双向鉴别。由于 7.2.2 给出的 scope 和 state 参数可能通过不安全信道传输,或被不安全存储,因此,不应以明文形式包含客户端或资源所有者的敏感信息。

#### B.2 重定向端点安全要求

任何与重定向端点的通信优先使用 B.1 给出的 TLCP。如 B.1 所述的 TLCP 不可用,授权服务器在重定向之前,应向资源所有者显示此端点不安全的警告。

不具备凭据保护能力的客户端在授权服务器上注册时,授权服务器宜要求其登记重定向端点:授权服务器宜要求所有类型的客户端在使用授权端点之前向授权服务器注册客户端的重定向端点。

授权服务器应要求客户端提供完整的重定向端点 URI。如客户端无法实现注册完整的重定向端点 URI,授权服务器宜要求客户端在注册时提供注册方案、主机名和路径等三部分(在客户端请求授权时只准许其变更重定向端点 URI 的查询组件)。

授权服务器允许客户端注册多个重定向端点。

如客户端注册了多个重定向端点 URI,或者只注册了重定向端点 URI 的一部分,或者没有注册重定向端点 URI,客户端在发送授权请求时,宜在请求中使用 redirect\_uri 参数来标识该次请求所使用的重定向端点 URI。

当授权请求中包含重定向端点 URI 时,如客户端注册过重定向端点 URI,授权服务器对收到的重定向端点 URI 和之前注册过的重定向端点 URI 进行比较和匹配。

如授权请求由于重定向端点 URI 丢失、无效或者不匹配而未通过验证,授权服务器宜告知资源所有者这一错误,并且不应自动将用户代理重定向到未通过验证的重定向端点 URI。

发向客户端重定向端点的重定向请求通常会获得 HTML 文档的响应,该响应由用户代理处理。客户端不宜在重定向请求的响应中包含任何第三方的脚本。客户端宜从重定向请求的 URI 中解析出凭据并将用户代理再次重定向到另外的端点,以避免凭据在 URI 中或其他地方被获取。

#### B.3 客户端身份鉴别安全要求

具备凭据保护能力的客户端和授权服务器之间应确立一种符合授权服务器安全要求(通常由授权服务器的服务文档提供)的身份鉴别方法,使得授权服务器可安全地对客户端的身份进行鉴别。授权服务器通常在具备凭据保护能力的客户端注册时,授予客户端身份凭据,通过基于身份凭据或数字证书的鉴别方案对客户端进行身份鉴别。具备凭据保护能力的客户端应保护其身份凭据的机密性和完整性。

不具备凭据保护能力的客户端可与授权服务器协商身份鉴别方法,但由于不具备凭据保护能力客户端无法保证凭据的机密性,授权服务器不应仅依赖该方法对客户端身份的真实性进行判定。

授权服务器不应发放客户端身份凭据给不具备凭据保护能力的客户端。但特殊设备上的本地应用如具有对身份凭据的保护能力,授权服务器可发放客户端身份凭据给该类客户端。

为了防止假冒的客户端,授权服务器应对客户端的身份进行鉴别。当客户端身份鉴别流程无法实施时,授权服务器应采用其他方式来验证客户端的身份。例如,授权服务器可要求客户端注册重定向端点并将请求中的重定向端点 URI 与注册的重定向端点 URI 进行对比,或者要求资源所有者参与确认客户端的身份(授权服务器鉴别资源所有者的身份后,将客户端及其请求的受保护资源访问范围与有效时间提供给资源所有者,由资源所有者检查当前客户端的信息,并决定授权或拒绝该请求)。验证重定向端点 URI 的有效性并要求资源所有者参与到鉴别流程中的方式,不足以验证客户端身份,但可防止将凭据传递给假冒的客户端。

如下 2 种情况授权服务器不应自动处理(未与资源所有者主动交互的情况下)重复的授权请求:

- a) 未鉴别客户端;
- b) 不能确认重复请求是来自真实的客户端,而不是假冒的客户端。

授权服务器应根据与未授权客户端交互的安全性,并采取措施以规避所发放的凭据(如刷新令牌)存在的暴露风险。

客户端在同一个请求中只准许使用一种身份鉴别方案。

#### B.4 授权码流程中的安全要求

在授权码流程中,安全要求如下。

- a) 授权码应使用 GB/T 38636 中规定的 TLCP 传输。
- b) 在发放授权码时,如授权服务器可鉴别客户端,则授权服务器鉴别该客户端,实现授权码发放给正确的客户端。
- c) 授权码为一次性有效,且授权码具有较短的生存周期。如授权服务器发现某个授权码被多次使用,授权服务器撤销利用该授权码发放的所有访问令牌(或和刷新令牌)。
- d) 当使用授权码许可类型时,客户端通过 `redirect_uri` 参数指定重定向端点 URI。如攻击者篡改重定向端点 URI 的值,将导致授权服务器把资源所有者的用户代理重定向到攻击者控制的端点(重定向请求中包含授权码)。为了避免此类攻击,授权服务器应验证用于获取授权码的重定向端点 URI 与用授权码获取访问令牌时提供的重定向端点 URI 是否一致。授权服务器应要求不具备凭据保护能力的客户端注册重定向端点 URI,宜要求具备凭据保护能力的客户端注册其重定向端点 URI。如请求中包含重定向端点 URI,授权服务器应根据注册值进行验证。

#### B.5 客户端身份凭据许可流程中的安全要求

客户端身份凭据许可流程中,安全要求如下。

- a) 授权服务器应要求客户端提前注册,注册完成后,授权服务器将生成的客户端身份凭据发放给客户端。客户端的身份凭据应能抵抗猜测攻击。
- b) 仅具备凭据保护能力的客户端应使用客户端身份凭据许可类型。

#### B.6 设备授权许可机制中的安全要求

设备授权许可机制中,安全要求如下:

- a) 由于用户码需要由用户输入,出于可用性考虑,较短的代码更为理想,意味着其熵较低,宜限制用户码在一定时间内的尝试次数;
- b) 用户码的确切长度和包含的熵由授权服务器自行决定,授权服务器需要考虑其特定受保护资源的敏感性、代码长度的实用性以及任何现有的缓解措施来确定用户代码的格式。

#### B.7 访问令牌安全要求

在传输和存储访问令牌时,应采取措施保护保证访问令牌(以及其他机密的访问令牌属性)的机密

性,并只在授权服务器、访问令牌规定范围的资源所在的资源服务器和访问令牌对应的客户端等三者中共享。访问令牌的传输应采用 GB/T 38636 规定的 TLCP。

客户端应根据需求请求最低的受保护资源访问范围的访问令牌。授权服务器应根据客户端的身份,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客户端请求的受保护资源访问范围。

为了防止访问令牌猜测攻击,授权服务器应保证攻击者单次尝试的成功概率不高于  $2^{-128}$ 。

## B.8 刷新令牌安全要求

在传输和存储刷新令牌时,应保证刷新令牌的机密性,并只在授权服务器、刷新令牌对应的客户端二者中共享。授权服务器应维护刷新令牌和接收刷新令牌的客户端之间的绑定关系。刷新令牌的传输应采用 GB/T 38636 规定的 TLCP。

在鉴别客户端的身份时,授权服务器应验证刷新令牌和客户端身份间的绑定关系。当无法鉴别客户端身份时,授权服务器应采用其他方式来检测刷新令牌是否被滥用。例如,授权服务器可采用刷新令牌环,刷新令牌环中新刷新令牌的发放对应每一个访问令牌的刷新请求。过期的刷新令牌失效但仍由授权服务器保存。如刷新令牌被盗用,且随后被攻击者和合法客户端使用,合法方将通过出示已失效的刷新令牌来向授权服务器证明自己的合法性。

授权服务器应采取措施防止未授权构造、修改刷新令牌,或通过猜测生成有效的刷新令牌。

为了防止刷新令牌猜测攻击,授权服务器应保证攻击者单次尝试的成功概率不高于  $2^{-128}$ 。



参 考 文 献

[1] GB/T 15843.3—2023 信息技术 安全技术 实体鉴别 第3部分:采用数字签名技术的机制

[2] GB/T 15852.2—2024 网络安全技术 消息鉴别码 第2部分:采用专门设计的杂凑函数的机制

[3] RFC 3986. Uniform Resource Identifier (URI): Generic Syntax. IETF, January 2005.

[4] RFC 5849. The OAuth 1.0 Protocol. IETF, April 2010.

[5] RFC 6749. The OAuth 2.0 Authorization Framework. IETF, October 2012.

[6] RFC 6750. The OAuth 2.0 Authorization Framework: Bearer Token Usage. IETF, October 2012.

[7] RFC 7522. Security Assertion Markup Language (SAML) 2.0 Profile for OAuth 2.0 Client Authentication and Authorization Grants. IETF, May 2015.

[8] RFC 7578. Returning Values from Forms: multipart/form-data. IETF, July 2015.

[9] RFC 7636. Proof Key for Code Exchange by OAuth Public Clients. IETF, September 2015.

[10] RFC 8446. The Transport Layer Security (TLS) Protocol Version 1.3. IETF, August 2018.

[11] RFC 8628. OAuth 2.0 Device Authorization Grant. IETF, August 2019.

[12] RFC 9110. HTTP Semantics. IETF, June 2022.

[13] RFC 9112. HTTP/1.1. IETF, June 2022.

[14] RFC 9700. OAuth 2.0 Security Best Current Practice. IETF, January 2024.

[15] Draft-ietf-oauth-v2-1-13. The OAuth 2.1 Authorization Framework. IETF, October 2025.

---



