ICS 35.030
CCS L 80

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

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、杨昫、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。