ICS 35.040
L 80

中华人民共和国密码行业标准

GM/T 0068—2019

开放的第三方资源授权协议框架

Open third party resource authorization protocol framework

2019-07-12 发布　　2019-07-12 实施

国家密码管理局　　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 …… 2
5　概述 …… 3
5.1　协议流程 …… 3
5.2　协议通道要求 …… 4
5.3　协议端点 …… 4
6　第三方应用程序及安全要求 …… 6
6.1　第三方应用程序类型 …… 6
6.2　第三方应用程序标识符 …… 7
6.3　第三方应用程序注册要求 …… 7
6.4　第三方应用程序身份鉴别 …… 7
7　授权流程 …… 8
7.1　授权许可 …… 8
7.2　授权码许可流程 …… 9
7.3　隐式许可流程 …… 12
7.4　资源拥有者口令凭据许可流程 …… 15
7.5　第三方应用程序身份凭据许可流程 …… 17
8　令牌 …… 18
8.1　令牌类型 …… 18
8.2　访问令牌发放 …… 20
8.3　访问令牌刷新 …… 21
9　受保护资源访问 …… 21
9.1　受保护资源访问流程 …… 21
9.2　成功响应 …… 22
9.3　出错响应 …… 22
附录A（资料性附录）　协议参数说明 …… 23
参考文献 …… 25

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准参考国际互联网工程任务组(The Internet Engineering Task Force,简称 IETF)的 RFC 6749 文件《The OAuth2.0 Authorization Framework》进行制定。按照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,本标准在第三方应用程序身份鉴别部分增加了基于 SM2 国产密码算法的数字证书鉴别方法,在授权协议中的数据通信安全部分采用密码行业标准 GM/T 0024—2014《SSL　VPN　技术规范》中定义的安全通信协议取代 TLS 协议,在访问令牌的保护部分增加了采用 SM2、SM3、SM4 等国家密码管理局认可的算法对其进行签名和加密的规定。另外,本标准去除了RFC 6749文件中的安全考虑部分,将安全考虑部分涉及的应采用的安全措施具体化到本标准的各个章条,包括协议中传输的消息、端点、发放的令牌、第三方应用程序身份鉴别等部分。

本标准由密码行业标准化技术委员会提出并归口。

本标准的主要起草单位: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、中国科学院软件研究所、中国电子技术标准化研究院、北京信安世纪科技股份有限公司、普华诚信信息技术有限公司。

本标准主要起草人:刘丽敏、李敏、王鑫、江伟玉、高能、刘宗斌、荆继武、林雪焰、张立武、汪宗斌、彭佳、屠晨阳、刘泽艺、钱文飞、范科峰、郝春亮、梁佐泉。

引　言

在提供了资源互访接口的开放信息系统中，利用 Web、桌面、手机或其他智能设备应用程序实现互联已成为常态。为了实现信息资源共享、业务合作，用户可利用某个安全域中的应用程序（被称为第三方应用程序）访问另一个安全域中受保护的资源。为了确保受保护的资源只被资源拥有者许可的实体访问，需要对实体进行鉴别与授权。然而，在传统的授权模型中，资源拥有者通常需要将其身份凭证共享给访问者，这种方式带来了诸多安全隐患。本标准引入授权层，将第三方应用程序与资源拥有者的角色进行分离，在资源拥有者的授权下，授权实体向第三方应用程序发放不同于身份凭据的令牌方式，实现开放的第三方资源授权。

开放的第三方资源授权协议框架

1 范围

本标准规定了第三方资源授权协议的流程、不同类型的授权许可、协议各端点的功能要求以及系统实体之间传递消息的格式和参数要求等。

本标准适用于在互联网跨安全域应用场景中，身份鉴别与授权服务的开发、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 15843.3—2008 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

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

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

RFC 2616 超文本传输协议 HTTP1.1(Hypertext Transfer Protocol—HTTP/1.1)

RFC 2617 HTTP鉴别：基本访问鉴别和摘要访问鉴别(HTTP Authentication：Basic and Digest Access Authentication)

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

RFC 6749 OAuth 2.0授权框架(The OAuth 2.0 Authorization Framework)

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

授权 authorization

授予访问者访问受保护资源的权限。

3.3

授权码 authorization code

授权服务器发放给第三方应用程序的凭据，表明资源拥有者同意第三方应用程序访问受保护资源，第三方应用程序可使用授权码获取访问令牌和刷新令牌。

3.4

授权端点 authorization endpoint

授权服务器上用于与资源拥有者交互的端点，用于接收资源拥有者的身份凭据和授权，以及返回授