ICS 35.040
L 80

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)