ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31504—2015

信息安全技术　鉴别与授权　数字身份信息服务框架规范

Information security technology—Authentication and authorization—Digital identity information service framework specification

2015-05-15 发布　　2016-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国科学院软件研究所、中兴通讯股份有限公司、北京信息科学技术研究院。

本标准主要起草人:冯登国、张敏、张立武、张妍、付艳艳、段美姣、张严、李强。

引　言

数字身份作为主体的虚拟标识，是其进行各种网络活动的支撑手段。数字身份管理是数字世界安全事务的核心，为鉴别、授权、访问控制、账户访问以及其他各种与用户属性应用提供支持。然而目前数字身份由各种服务提供方自行管理，不仅格式多样、管理混乱，而且不同服务提供方之间的身份信息难以交互，安全与隐私性也无法得到足够保障。因此迫切需要对我国数字身份管理技术进行规范化管理，使数字身份信息使用者可以准确地访问数字身份信息，身份提供方可以正确维护和管理数字身份信息，确保用户数字身份信息的安全和隐私。

本标准是数字身份管理规范化的基础性标准，致力于规范各种数字身份信息服务。本标准定义一种通用的可扩展的数字身份信息 XML Schema 框架与数字身份信息访问消息格式，支持多种类型的数字身份表示和访问，允许用户自定义格式扩展。支持数字身份信息的定义和访问过程的标准化，为各种类型的数字身份信息服务建立统一的服务框架规范。

本标准参考了 Liberty Alliance 的文件 Liberty ID-WSF Data Services Template v2.1。在原文件的基础上增加了对标准范围的说明以及数字身份信息参考模型部分。

信息安全技术　鉴别与授权
数字身份信息服务框架规范

1　范围

本标准定义了数字身份信息服务参考模型、XML Schema 的框架、命名空间、扩展方式以及通用的数字身份信息对象属性类型，还定义了通用的数字身份信息创建、查询、修改和删除的交换消息格式以及处理规则。

本标准适用于数字身份信息服务的开发，并可指导对该类系统的检测及相关应用的开发。

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 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 中界定的以及下列术语和定义适用于本文件。

3.1

账户　account

一个正式的商业协议，用于处理主体与一个服务提供方之间的交易和服务。

3.2

已鉴别身份　authenticated identity

一个已经被断言通过鉴别的主体的身份，可代表此主体。

3.3

鉴别　authentication

一个在指定级别的可信度下确定某主体声称的身份的过程。

3.4

鉴别权威　authentication authority

是鉴别身份提供方。一个可以鉴别某主体的身份提供方。

3.5

授权　authorization

根据对主体数字身份信息的评估，确定一个主体是否可以对资源实施指定类型的访问的过程。一旦某个主体被鉴别，就可能拥有某些类型的访问权限。

3.6

数字身份　digital identity

主体在互联网中的虚拟身份表示，关联了与该主体相关的属性信息，通常由一个账户标识其唯一性。