ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30275—2013

信息安全技术　鉴别与授权　认证中间件框架与接口规范

Information security technology—Authentication and authorization—Authentication middleware framework and interface specification

2013-12-31 发布　　2014-07-15 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。

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。

本文件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。

本标准主要起草单位:中国科学院软件研究所、中国科学院数据与通信保护研究教育中心、北京数字证书认证中心有限公司。

本标准主要起草人:徐静、冯登国、荆继武、张立武、张严、李强、杨婧、张振峰、詹榜华、阎实。

引　言

身份鉴别是保障系统安全的最基本功能之一，是绝大多数信息系统的首要安全需求。然而长期以来，安全功能与具体业务的紧密结合使得应用系统开发人员往往在考虑业务功能的同时还需要考虑安全功能的实现。因为不是所有的开发人员都具备全面的安全知识，这样做不仅费时费力，还不能保证安全功能的完整实施。因此，将安全功能，特别是身份鉴别功能与业务功能剥离，以中间件的方式为应用系统提供专门的安全保护，是安全领域的发展趋势。

此外，由于各个系统在建设过程中缺乏规范的鉴别接口和参考模型，不同系统之间互不兼容，无法互通互联，造成大量重复开发建设，浪费严重。同时更给进一步的系统集成工作带来困难。

因此，我国迫切需要制定认证中间件的框架及接口规范，对信息系统的鉴别过程进行标准化。从而提升信息系统的互操作能力，促进认证中间件的研发和推广，从宏观角度看来也将有助于推进我国信息安全保障体系建设。

本标准的主要目标是提供一套认证中间件的框架规范及其组件描述，并对鉴别实施过程予以规范，但为使本标准具有更好的可实现性与可操作性，本标准中同时对通用接口进行了若干定义，以便作为实现时的参考，这些定义不影响本标准中认证中间件框架的通用性。在实际应用中，可根据需求对这些接口进行进一步规范。

信息安全技术　鉴别与授权　认证中间件框架与接口规范

1　范围

本标准规定了认证中间件体系框架、组件、功能及通用接口，并给出了认证中间件的工作流程。

本标准适用于认证中间件及其组件的设计、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 9387.2—1995　信息处理系统　开放系统互连　基本参考模型　第2部分：安全体系结构

GB/T 15843.1—2008　信息技术　安全技术　实体鉴别　第1部分：概述

GB/T 18794.2—2002　信息技术　开放系统互连　开放系统安全框架　第2部分：鉴别框架

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 9387.2—1995、GB/T 15843.1—2008、GB/T 18794.2—2002 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

依赖方　relying party

根据从另一方实体处获得的信息来决定如何进行动作的系统实体。

注：例如应用系统依赖于认证中间件对用户进行身份鉴别。

3.2

断言　assertion

给依赖方的包含了用户身份信息的可信声明，也可以包含验证过的属性。

注：断言可能是经过数字签名的，或者是通过一个安全协议从可信源获取的。

3.3

属性　attribute

对象的性质及对象之间的关系的统称。

3.4

鉴别　authentication

在用户身份间建立信任的过程。

3.5

鉴别密钥协商　authenticated key agreement

两方或者两方以上的实体通过交互建立起彼此间身份的信任关系，并形成一个共同的秘密密钥，用于保护后续的通信安全。