ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31501—2015

信息安全技术　鉴别与授权　授权应用程序判定接口规范

Information security technology—Authentication and authorization—Specification for authorization application programming decision interface

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、北京数字证书鉴别中心有限公司、中科正阳信息安全技术有限公司。

本标准主要起草人:冯登国、张立武、李晓峰、王雅哲、高志刚、徐震、段美姣、汪丹、黄亮、翟征德、詹榜华。

引　言

访问控制作为一种基本的安全措施在实际系统中得到广泛的应用，随着访问控制技术的日趋复杂，访问控制已成为一类安全基础服务，而广泛的应用集成需求需要访问控制安全服务能够给应用程序提供一个统一的编程接口，使得应用程序能够在不同的访问控制服务之间具有可移植性，而目前缺少这类国家标准。为了解决这个问题，本标准参考了 Open Group 的技术标准（参考文献[1]）等相关标准和规范，在保证适应多种应用场景的情况下，定义了授权应用程序判定接口规范。

本标准定义的授权应用程序判定接口规范可用于符合 GB/T 18794.3 访问控制框架的系统中，尽管本标准提供了允许主体控制哪些特权属性可以被用于访问控制授权请求判定中（通常被称为最小特权），但并不提供特权属性管理。

本标准的设计目标如下：

a) 定义一个简单、灵活的 API，安全组件提供者和需要安全保护的应用程序开发者可以通过调用此 API 来实现授权功能；

b) 访问判定时可以应用透明地进行策略规则的评估；

c) 独立于应用的策略集中管理；

d) 透明地提供广泛的策略规则词法和语义（如访问控制列表、能力、标签、逻辑谓词等）；

e) 将鉴别和授权分离；

f) 允许从鉴别数据中推导出授权属性；

g) 透明地支持任意合理的授权属性类型（如访问标识、组、角色等）；

h) 易于在多层次结构的应用系统中提供授权服务；

i) 在多层应用配置中允许使用外部授权属性；

j) 应用程序可以访问应用于其资源的访问控制策略；

k) API 的实现支持多种访问控制机制；

l) 单一程序可以同时使用多个鉴别和授权服务；

m) 支持应用程序访问与授权服务操作相关的审计数据。

本标准不涉及以下内容：

a) 授权策略管理；

b) 描述证书委托服务或语义；

c) 描述一个审计服务 API；

d) 描述授权服务如何以及何时生成审计事件；

e) 在异构环境下，定义用来交换证书信息的 PAC 格式；

f) 支持每一种可能的授权策略规则词法和语义。

信息安全技术　鉴别与授权
授权应用程序判定接口规范

1　范围

本标准定义了访问控制服务为授权应用提供的授权判定编程应用接口，并定义了与判定接口相关的数据结构和C语言形式的接口。

本标准适用于访问控制服务中授权判定接口的设计和实现，访问控制服务的测试和产品采购亦可参照使用。

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 18794.3—2003　信息技术　开放系统互连　开放系统安全框架　第3部分：访问控制框架

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

访问控制信息　access control information

用于访问控制目的的任何信息，其中包括上下文信息。

[GB/T 18794.3—2003，定义3.4.5]

3.2

访问控制判定功能　access control decision function

一种特定功能，它通过对访问请求、ADI(发起者的、目标的、访问请求的或以前决策保留下来的ADI)以及该访问请求的上下文，使用访问控制策略规则而做出访问控制判定。

[GB/T 18794.3—2003，定义3.4.3]

3.3

访问控制判定信息　access control decision information

在作出一个特定访问控制判定时可供ADF使用的部分(也可能是全部)ACI。

[GB/T 18794.3—2003，定义3.4.2]

3.4

访问控制实施功能　access control enforcement function

一种特定功能，它是每一访问请求中发起者和目标之间访问路径的一部分，并实施由ADF做出的决策。

[GB/T 18794.3—2003，定义3.4.4]