



中华人民共和国国家标准

GB/T 36960—2018

信息安全技术 鉴别与授权 访问控制中间件框架与接口

Information security technology—Authentication and authorization—
Access control middleware framework and interface

2018-12-28 发布

2019-07-01 实施

国家市场监督管理总局
中国国家标准化管理委员会 发布

目 次

前言	I
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 访问控制中间件体系框架	3
5.1 概述	3
5.2 组件定义	4
5.3 组件间接口	7
5.4 接口间工作过程	8
6 访问控制中间件接口	9
6.1 概述	9
6.2 常量定义	9
6.3 策略决策接口(IF-PD)	9
6.4 决策管理接口(IF-DM)	9
6.5 策略查询接口(IF-PQ)	16
6.6 属性查询接口(IF-AQ)	22
6.7 跨域属性查询接口(IF-CDAQ)	26
附录 A (资料性附录) 应用场景	30
附录 B (资料性附录) 接口消息示例	32
参考文献	39

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。

本标准主要起草人:张严、张立武、高志刚、王鹏翮、冯登国、荆继武、吴槟、李强、林雪焰、陈星、高能、阎实。

信息安全技术 鉴别与授权 访问控制中间件框架与接口

1 范围

本标准确立了鉴别与授权系统中访问控制中间件的框架结构与内部组件关系,规定了访问控制中间件中各组件的功能、操作流程及接口要求。

本标准适用于访问控制中间件及其内部组件的设计与实现,并可指导对该类中间件系统的检测及相关应用的开发,对该类中间件产品的采购亦可参照使用。

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 13000 信息技术 通用多八位编码字符集(UCS)

GB/T 18793—2002 信息技术 可扩展置标语言(XML)1.0

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

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

3 术语和定义

GB/T 25069—2010、GB/T 18794.3—2003 界定的以及下列术语和定义适用于本文件。

3.1

访问控制中间件 access control middleware

通过对适用的访问控制信息进行评估以决定发起者是否可以对访问目标进行特定类型访问的一系列组件及组件间接口的集合。

3.2

动作 action

访问控制行为发起者执行的某种操作。

注:例如读取、修改、删除等。

3.3

属性 attribute

主体、资源、动作和环境的某个特征,该特征可以在策略中被引用。

3.4

决策 decision

依据访问控制策略做出的判定结果。

注:例如允许或拒绝用户访问特定资源。