ICS 35.100.01
L 79

中华人民共和国国家标准

GB/T 18794.3—2003/ISO/IEC 10181-3:1996

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

Information technology—Open Systems Interconnection—
Security frameworks for open systems—
Part 3:Access control framework

(ISO/IEC 10181-3:1996,Information technology—
Open Systems Interconnection—
Security frameworks for open systems:
Access control framework,IDT)

2003-11-24 发布　　2004-08-01 实施

中华人民共和国
国家质量监督检验检疫总局　发布

GB/T 18794.3—2003/ISO/IEC 10181-3:1996

中华人民共和国
国家标准
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 18794.3—2003/ISO/IEC 10181-3:1996
*
中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045
网址 www.bzcbs.com
电话:68523946　68517548
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230　1/16　印张 2.75　字数 73千字
2004年5月第一版　2004年5月第一次印刷
*
书号:155066·1-20583　定价 19.00 元

GB/T 18794.3-2003

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 2
3　术语和定义 …… 2
4　缩略语 …… 5
5　访问控制的一般性论述 …… 5
5.1　访问控制的目标 …… 5
5.2　访问控制的基本方面 …… 5
5.2.1　执行访问控制功能 …… 6
5.2.2　其他访问控制活动 …… 7
5.2.3　ACI 转发 …… 9
5.3　访问控制组件的分布 …… 9
5.3.1　入访问控制 …… 10
5.3.2　出访问控制 …… 10
5.3.3　插入访问控制 …… 10
5.4　跨多个安全域的访问控制组件分布 …… 10
5.5　对访问控制的威胁 …… 10
6　访问控制策略 …… 11
6.1　访问控制策略表示 …… 11
6.1.1　访问控制策略分类 …… 11
6.1.2　组和角色 …… 11
6.1.3　安全标签 …… 11
6.1.4　多个发起者的访问控制策略 …… 12
6.2　策略管理 …… 12
6.2.1　固定的策略 …… 12
6.2.2　行政管理强加的策略 …… 12
6.2.3　用户选择的策略 …… 12
6.3　粒度和容度 …… 12
6.4　继承规则 …… 12
6.5　访问控制策略规则中的优先原则 …… 13
6.6　默认访问控制策略规则 …… 13
6.7　通过合作安全域的策略映射 …… 13
7　访问控制信息和设施 …… 13
7.1　ACI …… 13
7.1.1　发起者 ACI …… 13
7.1.2　目标 ACI …… 14
7.1.3　访问请求 ACI …… 14
7.1.4　操作数 ACI …… 14
7.1.5　上下文信息 …… 14

7.1.6 发起者绑定 ACI …… 14
7.1.7 目标绑定 ACI …… 14
7.1.8 访问请求绑定 ACI …… 15
7.2 ACI 的保护 …… 15
7.2.1 访问控制证书 …… 15
7.2.2 访问控制权标 …… 15
7.3 访问控制设施 …… 15
7.3.1 与管理相关的设施 …… 16
7.3.2 与操作相关的设施 …… 16
8 访问控制机制分类 …… 18
8.1 引言 …… 18
8.2 访问控制列表(ACL)方案 …… 19
8.2.1 基本特性 …… 19
8.2.2 ACI …… 19
8.2.3 支持机制 …… 19
8.2.4 方案的变种 …… 20
8.3 权力方案 …… 21
8.3.1 基本特性 …… 21
8.3.2 ACI …… 21
8.3.3 支持机制 …… 21
8.3.4 方案变种——不带具体操作的权力 …… 22
8.4 基于标签的方案 …… 22
8.4.1 基本特性 …… 22
8.4.2 ACI …… 22
8.4.3 支持机制 …… 22
8.4.4 将信道标记为目标 …… 23
8.5 基于上下文的方案 …… 23
8.5.1 基本特性 …… 23
8.5.2 ACI …… 23
8.5.3 支持机制 …… 24
8.5.4 方案变种 …… 24
9 与其他安全服务和机制的交互 …… 24
9.1 鉴别 …… 24
9.2 数据完整性 …… 24
9.3 数据机密性 …… 24
9.4 审计 …… 24
9.5 其他与访问相关的服务 …… 25
附录 A（资料性附录） 组件间访问控制证书的交换 …… 26
附录 B（资料性附录） OSI 参考模型中的访问控制 …… 28
附录 C（资料性附录） 访问控制身份的非惟一性 …… 29
附录 D（资料性附录） 访问控制组件的分布 …… 30
附录 E（资料性附录） 基于规则策略与基于身份策略的比较 …… 33
附录 F（资料性附录） 支持通过发起者转发 ACI 的机制 …… 34
附件 G（资料性附录） 访问控制安全服务概要 …… 35

附 录 G
（资料性附录）
访问控制安全服务概要

<table>
<tr><td colspan="2" rowspan="2">安全服务概要</td><td>元素</td><td>实体：发起者、目标</td><td></td><td></td></tr>
<tr><td></td><td>功能：访问控制实施功能(AEF)
访问控制判决功能(ADF)
信息：访问控制信息(ACI)、访问控制判决信息(ADI)、
上下文信息、策略规则</td><td></td><td></td></tr>
<tr><td colspan="2"></td><td colspan="4">实体目标：对信息进行解释，允许发起者只作为被授权者访问目标</td></tr>
<tr><td rowspan="8">设施</td><td>实体</td><td colspan="4">安全域机构(SDA)</td></tr>
<tr><td>功能</td><td colspan="4"></td></tr>
<tr><td>与管理相关的设施</td><td colspan="4">——安装 ACI
——改变 ACI
——撤销 ACI
——撤销 ADI
——列表 ACI
——禁用组件
——重新启用组件</td></tr>
<tr><td>实体</td><td>发起者</td><td>目标</td><td colspan="2"></td></tr>
<tr><td>功能</td><td></td><td></td><td colspan="2">ADF</td></tr>
<tr><td>与操作相关的设施</td><td>——识别远程授权机构
——建立安全交互策略
——获取 ACI
——生成 ACI
——撤销 ADI</td><td>——获取 ACI
——撤销 ADI</td><td colspan="2">——获取 ACI
——验证 ACI 和导出 ADI
——获取上下文的 ACI
——判决访问</td></tr>
<tr><td rowspan="3">信息</td><td>SDA 管理的数据元素</td><td colspan="4">——标识符(SDA、发起者、目标、安全交互策略、组、角色)
——ACI 选择准则
——有效期
——敏感性标记
——完整性标记</td></tr>
<tr><td>操作中使用的信息</td><td colspan="4">——ACI/ADI(发起者、发起者绑定、目标、目标绑定、访问请求、访问请求绑定、操作数、操作数绑定、交换、上下文、保留)
——访问控制列表
——权力
——标签
——访问控制证书
——访问控制权标</td></tr>
<tr><td>控制消息</td><td colspan="4">——时间周期
——系统状态
——访问控制策略表示
——鉴别强度
——通信路由</td></tr>
</table>