

ICS 35.240

A 90

# GF

公安部计算机信息系统安全产品质量监督检验中心检验规范

MSTL\_JGF\_04-010 0101—2006

---

## 信息安全技术 访问控制产品检验规范

2006-01-01 发布

2006-02-01 实施

---

公安部计算机信息系统安全产品质量监督检验中心 发布



## 目 次

前 言 .....	II
1 范围 .....	1
2 规范性引用文件 .....	1
3 术语和定义 .....	1
4 产品安全功能要求 .....	1
4.1 访问控制功能要求 .....	1
4.2 自身安全功能要求 .....	1
4.3 日志功能要求 .....	2
5 产品安全保证要求 .....	2
6 访问控制安全功能的等级划分 .....	3

## 前 言

为了规范全国访问控制产品的开发与应用，保障公共信息网络安全，根据公安部公共信息网络安全监察局的要求，本规范对访问控制产品提出了安全功能要求和保证要求，作为对其进行检测的依据。

本规范由中华人民共和国公安部公共信息网络安全监察局批准。

本规范起草单位：公安部计算机信息系统安全产品质量监督检验中心。

公安部计算机信息系统安全产品质量监督检验中心负责对本规范的解释、提升和更改。

# 信息安全技术 访问控制产品检验规范

## 1 范围

本规范规定了访问控制产品的安全功能要求和安全保证要求。

本规范适用于访问控制产品的开发及检测。

## 2 规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第3部分：安全保证要求（idt ISO/IEC 15408-3:1999）

## 3 术语和定义

### 3.1 访问控制 Access Control

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证系统资源不被非法使用和访问，使用访问控制的目的在于通过限制用户对特定资源的访问保护系统资源。

## 4 产品安全功能要求

### 4.1 访问控制功能要求

#### 4.1.1 用户鉴别机制

在用户请求访问受保护资源前必须进行身份鉴别，由系统对请求者身份进行确认。

#### 4.1.2 访问保障能力

授权用户能够根据预定义的策略访问相应资源。

#### 4.1.3 访问限制能力

- a) 访问用户限制：只有授权用户能够对受保护资源进行访问；
- b) 访问内容限制：授权用户对受保护资源进行访问的内容不能超出预定义的范围；
- c) 访问动作限制（有则适用）：授权用户对受保护资源进行访问的动作（如对文件进行只读、写、执行、属性修改、重命名、删除和移动等操作）不能超出预定义的允许范围；
- d) 访问时间限制（有则适用）：授权用户对受保护资源进行访问的时间不能超出预定义的范围；
- e) 访问地址限制（有则适用）：远程授权用户通过网络对受保护资源进行访问，该用户所在地址不能超出预定义的范围；
- f) 访问次数限制（有则适用）：授权用户对受保护资源进行访问的次数不能超出预定义的范围

#### 4.1.4 安全策略不可旁路

访问控制产品应确保用户对受保护资源的访问都要受到安全策略的制约。

### 4.2 自身安全功能要求

#### 4.2.1 符合规定的加密操作（有则适用）

- a) 如果支持远程管理，应能够通过加密等方式来保护远程管理对话内容不被非授权获取；
- b) 如果用户必须通过网络访问特定信息，应能够通过加密来保护远程访问会话。

#### 4.2.2 访问控制项目管理

##### 4.2.2.1 用户管理

访问控制产品应可以对用户进行管理，可以创建、修改和删除用户。

#### 4.2.2.2 资源管理

访问控制产品应可以对被访问控制产品控制访问的资源进行管理，可以增加和减少资源。

#### 4.2.2.3 用户角色管理

访问控制产品应能对用户进行分级（分权）角色管理，可以建立具有不同级别的角色，并可以针对各个角色设定不同的访问权限。

#### 4.2.3 管理员鉴别机制

访问控制产品应确保在授权管理员执行与访问控制产品安全相关的任何操作之前，必须经过身份鉴别。

#### 4.2.4 管理员权限

##### 4.2.4.1 管理员属性修改

访问控制产品应保证授权管理员的属性（至少包括管理员口令）能够修改。

##### 4.2.4.2 配置管理能力

访问控制产品应保证授权管理员能配置和管理访问控制产品安全相关的所有功能，至少应该包括：

- a) 系统状态定制；
- b) 增加、删除和修改访问控制策略；
- c) 查阅当前策略配置；
- d) 查阅和管理日志资料。

#### 4.2.5 管理角色

产品安全功能应划分不同的安全管理角色，对产品进行合理的权限分配。

#### 4.2.6 身份鉴别时效和失败处理

当用户的失败登录次数超过允许的尝试鉴别次数时，应能加以检测，并应该阻止该用户的进一步登录尝试，直至授权管理员恢复对该用户的鉴别能力。

#### 4.2.7 本地 agent 的自身保护功能（有则适用）

- a) 应采取防止非授权用户强行终止agent程序运行的措施；
- b) 应采取防止非授权用户强制取消agent程序在系统启动时自动加载的措施；
- c) 应采取防止非授权用户强行卸载、删除或修改agent程序的措施。

### 4.3 日志功能要求

#### 4.3.1 日志数据生成

应能对下列事件生成日志记录：

- a) 管理员鉴别机制的使用；
- b) 用户的鉴别机制的使用；
- c) 用户访问被保护资源的行为。

应在每一个日志记录中记录事件发生的日期和时间、事件主体身份、事件描述，成功或失败的标志。

#### 4.3.2 可理解的格式

访问控制产品应确保日志记录的内容可为人所理解。

#### 4.3.3 日志跟踪管理

访问控制产品应提供对日志记录的存档、删除和清空功能。

#### 4.3.4 限制日志访问

- a) 访问控制产品应只允许授权管理员访问日志记录；
- b) 访问控制产品应提供具有查阅日志数据能力的工具；
- c) 访问控制产品应提供对日志数据的进行条件查询的工具。

## 5 产品安全保证要求

保证要求按 GB/T 18336.3—2001 第二级执行。

## 6 访问控制安全功能的等级划分

根据信息技术-访问控制产品的开发、生产现状及实际应用情况，访问控制产品的安全功能要求划分成二个等级。

访问控制产品安全技术要求等级划分如表1所示。

表 1 访问控制产品安全功能等级划分表

安全功能类	基本要求	增强要求
4.1.1 用户鉴别机制	√	√
4.1.2 访问保障能力	√	√
4.1.3 访问限制能力	√	√
4.1.4 安全策略不可旁路	√	√
4.2.1 符合规定的加密操作	√	√
4.2.2.1 用户管理	√	√
4.2.2.2 资源管理	√	√
4.2.2.3 用户角色管理		√
4.2.3 管理员鉴别机制	√	√
4.2.4.1 管理员属性修改	√	√
4.2.4.2 配置和管理能力	√	√
4.2.5 管理角色		√
4.2.6 身份鉴别时效和失败处理		√
4.2.7 本地 agent 的自身保护功能	√	√
4.3.1 日志数据生成	b)	√
4.3.2 可理解的格式	√	√
4.3.3 日志跟踪管理		√
4.3.4 限制日志跟踪访问	a) 、 b)	√
保证要求	√	√
基本要求：为访问控制产品的最低安全级别。		
增强要求：为进一步提升产品安全功能的附加要求。		