

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_04-009

信息安全技术 文件加密产品检验规范

(第三版)

2006-08-07 发布

2006-08-021 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 安全功能..... | 1 |
| 4.2 日志审计功能..... | 1 |
| 4.3 密钥管理功能..... | 2 |
| 5 产品安全保证要求 | 2 |
| 6 文件加密产品安全功能的等级划分 | 2 |

前 言

为了规范全国文件加密产品的开发与应用，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，本规范对文件加密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 文件加密产品检验规范

1 范围

本规范规定了文件加密产品的安全功能要求和安全保证要求。
本规范适用于文件加密产品的开发及检测。

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 文件加密 file encrypt

文件加密是指使用加密技术对文件或目录进行保护。

4 产品安全功能要求

4.1 安全功能

4.1.1 对文件的加、解密

应能对授权用户选择的任意文件进行加、解密。

4.1.2 对目录的加、解密

应能对授权用户选择的任意目录进行加、解密。

4.1.3 加密文件的完整性校验

对于加密后的文件，文件加密产品应对其完整性进行校验。

4.1.4 加密文件的完整性恢复

对于被破坏的加密文件，文件加密产品应可根据加密文件中的冗余数据在一定程度内恢复加密文件的完整性。

4.1.5 加密文件、目录密钥更新功能

应提供对于已加密的文件和目录的密钥更新功能，产品应可自动更换已加密文件和目录的加密密钥。

4.1.6 运算空间保证

对文件或目录的加、解密运算应在私有空间内完成。

4.1.7 身份鉴别

用户在使用产品的安全功能之前应进行身份鉴别。

4.1.8 备份

若使用密码算法的密钥库，则应提供密钥库的备份功能。

4.2 日志审计功能

4.2.1 身份鉴别

应对用户的身份鉴别过程进行审计跟踪，包括鉴别成功和失败。

4.2.2 文件、目录加解密

应对文件和目录的加、解密过程进行审计跟踪。

4.2.3 密钥管理

若产品的密钥管理功能涉及密钥的管理过程，则应对密钥管理过程进行审计跟踪。至少包括：密钥生成、密钥更新、密钥销毁。

4.3 密钥管理功能

4.3.1 密码算法

产品提供的密码算法应符合国家密码管理的有关规定。

4.3.2 密钥生成

产品应可根据密钥管理规定，生成符合规定的密钥。

4.3.3 密钥的分发或注入

应说明所使用密钥（对称密钥或非对称密钥）的分发或注入方法。

4.3.4 密钥更新

应说明所使用密钥的更新方法。

4.3.5 密钥归档

应说明所使用密钥的归档方法。

4.3.6 密钥恢复

应说明是否提供密钥恢复功能以及所使用的密钥恢复方法。

4.3.7 密钥销毁

对于不再使用的密钥，产品应提供密钥销毁功能。

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 文件加密产品安全功能的等级划分

依据文件加密产品的开发、生产现状及实际应用情况，我们对文件加密类产品的安全功能要求划分成二个等级。

文件加密产品安全功能的等级划分如表 1 所示。

表1 文件加密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 对文件的加、解密 | √ | √ |
| 4.1.2 对目录的加、解密 | | √ |
| 4.1.3 加密文件的完整性校验 | | √ |
| 4.1.4 加密文件的完整性恢复 | | √ |
| 4.1.5 加密文件、目录密钥更新功能 | | √ |

表1 （续）

| | | |
|--|---|---|
| 4.1.6 运算空间保证 | | √ |
| 4.1.7 身份鉴别 | √ | √ |
| 4.1.8 备份 | √ | √ |
| 4.2 日志和审计 | | √ |
| 4.3.1 密码算法 | √ | √ |
| 4.3.2 密钥生成 | | √ |
| 4.3.3 密钥的分发或注入 | √ | √ |
| 4.3.4 密钥更新 | | √ |
| 4.3.5 密钥归档 | | √ |
| 4.3.6 密钥恢复 | √ | √ |
| 4.3.7 密钥销毁 | | √ |
| <p>a 基本要求：为产品的最低安全级别。</p> <p>b 增强要求：为进一步提升产品安全功能的附加要求。</p> | | |