ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 988—2012

信息安全技术
文件加密产品安全技术要求

Information security technology—
Security technical requirements for file encryption products

2012-04-25 发布　　2012-04-25 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人：俞优、顾建新、顾健、赵婷、陆臻、沈亮、吴其聪、李毅、张笑笑、马海燕、顾玮、邹春明。

信息安全技术
文件加密产品安全技术要求

1 范围

本标准规定了文件加密产品的安全功能要求、自身安全功能要求、安全保证要求和等级划分要求。

本标准适用于文件加密产品的设计、开发及检测。

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 5271.8—2001 信息技术 词汇 第8部分：安全

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336.3—2008 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

3 术语和定义

GB/T 5271.8—2001、GB 17859—1999 和 GB/T 18336.3—2008 界定的以及下列术语和定义适用于本文件。

3.1

文件加密产品 file encryption products

使用密码技术对指定文件进行保护的产品，其中密码技术应符合国家密码管理相关规定。

3.2

密钥 key

一串符号序列，实现控制密码变换操作(加密、解密)的关键信息或参数。

3.3

密码算法 cryptographic algorithm

在密钥控制下的一簇数学运算，规定了完成数据加解密的程序的一系列规则，以实现明文和密文之间的相互变换。

4 安全功能要求

4.1 加、解密管理

4.1.1 文件加、解密

产品应实现下列加、解密功能：