ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 989—2012

信息安全技术
电子文档安全管理产品安全技术要求

Information security technology—Security technical requirements for security management products of electronic documents

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，深圳市虹安信息技术有限公司，北京鼎普科技股份有限公司。

本标准主要起草人：宋好好、张艳、顾健、赵云、张笑笑、吴其聪、邹春明、王志佳、张观纯、王江波。

信息安全技术
电子文档安全管理产品安全技术要求

1 范围

本标准规定了电子文档安全管理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。

本标准适用于电子文档安全管理产品的设计、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

安全电子文档 security electronic document

受到安全管理策略限制、保护的电子文档。

3.2

电子文档安全管理产品 security management products of electronic documents

通过制作安全电子文档或将电子文档转换为安全电子文档，对安全电子文档进行统一管理、监控和审计的产品。该类产品通过用户身份认证、访问控制、审计机制等管理手段，阻止对安全电子文档的非授权访问。

3.3

可信主机 trusted host

被电子文档安全管理产品授权可识别、访问安全电子文档的主机。

3.4

非可信主机 untrusted host

未被电子文档安全管理产品授权可识别、访问安全电子文档的主机。

4 安全功能要求

4.1 可信主机管理

4.1.1 可信主机注册

电子文档安全管理产品应能够将主机注册为可信主机。

4.1.2 可信主机分组

电子文档安全管理产品应能对可信主机进行分组，并能为不同分组的可信主机指定可以访问的安全电子文档。

4.1.3 可信主机注销

电子文档安全管理产品应能注销可信主机。

4.2 安全电子文档管理

4.2.1 安全电子文档生成

电子文档安全管理产品应能够依据安全管理策略制作安全电子文档或将电子文档转换为安全电子文档，转换过程中应保证电子文档内容的完整性。

4.2.2 安全管理策略

对安全电子文档的安全管理策略应包括以下要素：

a) 合法使用用户/用户组；
b) 内容是否限定为“只读”；
c) 使用期限；
d) 限制打开次数；
e) 是否允许打印以及打印次数限制；
f) 内容是否允许被修改；
g) 内容是否允许被复制；
h) 是否允许被转换生成电子文档。

4.2.3 安全管理策略管理

电子文档安全管理产品应能：

a) 导入、导出安全管理策略；
b) 定制安全管理策略模板。

4.2.4 安全管理策略查看

安全电子文档生成者应具备对该安全电子文档的安全属性进行查看的功能。

4.2.5 安全管理策略变更

安全电子文档生成者应具备对该安全电子文档的安全管理策略进行变更的功能。

4.3 安全电子文档认证

4.3.1 主机鉴别

在用户请求访问安全电子文档时，安全电子文档应对主机进行身份鉴别。

4.3.2 用户身份鉴别

在用户请求访问安全电子文档时，电子文档安全管理产品应鉴别用户身份。

若采用口令鉴别机制，应不明文显示口令。

4.3.3 最少反馈

对用户身份进行鉴别时，电子文档安全管理产品应仅将最少的反馈（如：输入的字符数，鉴别的成功或失败）提供给被鉴别的用户。

4.3.4 鉴别数据保护

电子文档安全管理产品应保证用户的鉴别数据不被未授权访问。

4.3.5 鉴别失败处理

电子文档安全管理产品应能为用户身份鉴别设定一个授权管理员可修改的鉴别尝试次数阈值，当用户鉴别不成功的次数超过阈值，产品应阻止用户进一步的鉴别请求。

4.3.6 超时锁定

安全电子文档应具有访问超时锁定功能。在设定的时间段内授权用户没有任何操作的情况下终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

4.3.7 会话锁定

电子文档安全管理产品应提供锁定授权用户与安全电子文档交互会话的功能，锁定后仅允许当前用户再次进行身份鉴别成功后才能够访问该安全电子文档。

4.4 安全标记

电子文档安全管理产品应能对所有的用户和安全电子文档设置敏感标记，并在产品安装后启用。

4.5 访问控制

4.5.1 自主访问控制

电子文档安全管理产品应能：

a) 允许授权用户在可信主机上访问安全电子文档的操作；
b) 拒绝在非可信主机上访问安全电子文档的操作；
c) 拒绝非授权用户在可信主机上访问安全电子文档的操作；
d) 执行自主访问控制策略，依据安全管理策略，控制授权用户在可信主机上对安全电子文档的访问。

4.5.2 强制访问控制

电子文档安全管理产品应能执行强制访问控制策略，通过比较安全标记、依据安全管理策略，控制授权用户在可信主机上对安全电子文档的访问。

4.5.3 安全管理策略不可旁路

电子文档安全管理产品应确保用户对受保护安全电子文档的访问都要受到安全管理策略的制约。

5 自身安全功能要求

5.1 组件安全

5.1.1 可信主机的自身保护功能

电子文档安全管理产品应能对安装在可信主机上的组件提供一定的保护措施，防止非授权用户进

行以下操作：

a) 强行终止该组件运行；

b) 强制取消该组件在系统启动时自动加载；

c) 强行卸载、删除或修改该组件。

5.1.2 防止非授权监控

应采取措施保证可信主机只接受授权管理控制台的监控。

5.1.3 远程传输安全

若电子文档安全管理产品组件间通过网络进行通讯，应对组件间传输的数据进行保护，保证在传送过程中数据的保密性和完整性。

5.2 管理员安全管理

5.2.1 标识与鉴别

5.2.1.1 管理员属性初始化

电子文档安全管理产品应提供授权管理员属性的初始化能力。

5.2.1.2 管理员唯一性标识

电子文档安全管理产品应为授权管理员提供唯一的身份标识，同时将授权管理员的身份标识与该授权管理员的所有可审计事件相关联。

5.2.1.3 管理员身份鉴别

电子文档安全管理产品应在执行任何与安全功能相关的操作之前鉴别任何声称要履行授权管理员职责的管理员身份。

5.2.1.4 管理员鉴别数据保护

电子文档安全管理产品应保证管理员的鉴别数据不被未授权访问。

5.2.1.5 管理员鉴别失败处理

当对授权管理员鉴别失败的次数达到指定阈值后，电子文档安全管理产品应阻止授权管理员进一步的鉴别请求。

5.2.2 安全管理角色

电子文档安全管理产品应能对管理员角色进行区分，提供以下功能实现基于不同角色的安全管理：

a) 具有至少两种不同权限的管理员角色；

b) 应根据不同的功能模块，自定义各种不同权限角色，并可对管理员分配角色。

5.2.3 管理员管理

电子文档安全管理产品应提供以下功能对管理员进行管理：

a) 创建和删除管理员；

b) 修改管理员的属性(包括管理员口令、管理员权限)。

5.3 用户安全管理

5.3.1 授权用户唯一性标识

电子文档安全管理产品应为授权用户提供唯一的身份标识，同时将授权用户的身份标识与该授权用户的所有可审计事件相关联。

5.3.2 用户管理

电子文档安全管理产品应具有对用户进行管理的功能，可以创建、修改和删除用户。

5.3.3 用户分组管理

电子文档安全管理产品应具有对授权用户进行分组管理的功能，可以创建、删除用户组，可以为用户组添加、修改和删除用户。

5.3.4 用户角色管理

电子文档安全管理产品应具有对授权用户进行分级(分权)角色管理的功能，可以建立具有不同级别的角色，并可以针对各个角色设置不同的用户权限。

5.4 审计功能

5.4.1 审计日志生成

电子文档安全管理产品应至少能对下列事件进行审计：

a) 授权管理员鉴别成功和失败；
b) 用户身份鉴别成功和失败；
c) 管理员鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；
d) 用户身份鉴别尝试不成功的次数超出了设定的限制导致会话连接终止；
e) 管理员的重要操作，如增加、删除管理员，用户管理，备份日志等；
f) 授权用户的重要操作，如制作安全电子文档、将电子文档转换为安全电子文档，制定、变更安全管理策略等；
g) 对安全电子文档访问的所有请求，包括成功和失败。

每一条审计日志至少应包括事件发生的日期、时间、用户标识、事件描述和事件结果(成功或失败)等。

5.4.2 审计日志存储

电子文档安全管理产品应提供以下功能对审计日志进行存储：

a) 存储在掉电非易失性存储介质中；
b) 当存储空间达到阈值时，应通知授权管理员。

5.4.3 审计日志管理

电子文档安全管理产品应提供以下功能对审计日志进行管理：

a) 只允许授权管理员访问审计日志；
b) 应能按日期、时间、用户标识、文件标识等条件对审计日志进行组合查询；
c) 应能对审计日志进行备份。

6 安全保证要求

6.1 配置管理

6.1.1 配置管理能力

6.1.1.1 版本号

开发者应为产品的不同版本提供唯一的标识。

6.1.1.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效维护的证据。

6.1.1.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

6.1.2 配置管理覆盖

配置管理范围至少应包括产品交付与运行文档、开发文档、指导性文档、生命周期支持文档、测试文档、脆弱性分析文档和配置管理文档，从而确保它们的修改是在一个正确授权的可控方式下进行的。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

6.2 交付与运行

6.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

6.2.2 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

6.3 开发

6.3.1 非形式化功能规范

开发者应提供一个功能规范，使用非形式化风格来描述产品安全功能及其外部接口。

功能规范应是内在一致的，应描述所有外部接口的用途与使用方法，适当时应提供效果、例外情况和错误消息的细节，并完备地表示产品的功能。

6.3.2 高层设计

6.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计。

高层设计应以非形式风格表述并且是内在一致的。为说明安全功能的结构，应将安全功能分解为各个安全功能子系统进行描述。对于每一个安全功能子系统，应描述其提供的安全功能，标识其所有接口以及哪些接口是外部可见的，描述其所有接口的使用目的和方法。高层设计还应标识安全功能要求的所有基础性的硬件、固件和软件，并且支持由这些硬件、固件和软件实现的保护机制。

6.3.2.2 安全加强的高层设计

开发者应阐明如何将有助于产品安全功能的子系统和其他子系统分开，并适当提供安全功能子系统的作用、例外情况和错误消息的细节。

6.3.3 非形式化对应性证实

开发者应在产品安全功能表示的所有相邻对之间提供对应性分析。

对于产品安全功能表示的每个相邻对，分析应阐明：较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备地细化。

6.4 指导性文档

6.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；

b) 怎样安全地管理产品；

c) 在安全处理环境中应被控制的功能和权限；

d) 所有对与产品的安全操作有关的用户行为的假设；

e) 所有受管理员控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；

g) 所有与管理员有关的 IT 环境安全要求。

6.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；

b) 产品提供给用户的安全功能和接口的使用方法；

c) 用户可获取受安全处理环境所控制的所有功能和权限；

d) 产品安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求。

6.5 生命周期支持

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，还应提供在产品的开发和维护过程中执行安全措施的证据。

6.6 测试

6.6.1 覆盖

6.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

6.6.1.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

6.6.2 测试深度

开发者应提供测试深度的分析。

在深度分析中，应说测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

6.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；

c) 预期的测试结果，应表明测试成功后的预期输出；

d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

6.6.4 独立测试

6.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

6.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

6.7 脆弱性分析保证

6.7.1 指南审查

开发者应提供指南性文档。

在指南性文档中，应确定对产品的所有可能的操作方式(包括失败或失误后的操作)、它们的后果以及对于保持安全操作的意义，还应列出所有目标环境的假设以及所有外部安全措施(包括外部程序的、物理的或人员的控制)要求。

指南性文档应是完备的、清晰的、一致的、合理的。

6.7.2 安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，说明该安全机制达到或超过指导性文档中定义的最低强度级别和特定功能强度度量。

6.7.3 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

7 等级划分要求

7.1 概述

依据电子文档安全管理相关产品的开发、生产现状及实际应用情况，将安全功能要求、自身安全功能要求和安全保证要求划分成三个等级。

7.2 安全功能要求等级划分

电子文档安全管理产品的安全功能要求等级划分如表1所示。

表1 电子文档安全管理产品安全功能要求等级划分

安全功能要求		第一级	第二级	第三级
可信主机管理	可信主机注册	4.1.1	4.1.1	4.1.1
	可信主机分组	—	4.1.2	4.1.2
	可信主机注销	4.1.3	4.1.3	4.1.3
安全电子文档管理	安全电子文档生成	4.2.1	4.2.1	4.2.1
	安全管理策略	4.2.2a)、4.2.2b)	4.2.2a)～4.2.2e)	4.2.2
	安全管理策略管理	—	4.2.3a)	4.2.3
	安全管理策略查看	—	—	4.2.4
	安全管理策略变更	—	—	4.2.5
安全电子文档认证	主机鉴别	4.3.1	4.3.1	4.3.1
	用户身份鉴别	4.3.2	4.3.2	4.3.2
	最少反馈	4.3.3	4.3.3	4.3.3
	鉴别数据保护	4.3.4	4.3.4	4.3.4
	鉴别失败处理	—	4.3.5	4.3.5

表 1（续）

安全功能要求		第一级	第二级	第三级
安全电子文档认证	超时锁定	—	4.3.6	4.3.6
	会话锁定	—	—	4.3.7
安全标记		—	—	4.4
访问控制	自主访问控制	4.5.1	4.5.1	4.5.1
	强制访问控制	—	—	4.5.2
	安全管理策略不可旁路	4.5.3	4.5.3	4.5.3

7.3 自身安全功能要求等级划分

电子文档安全管理产品的自身安全功能要求等级划分如表 2 所示。

表 2 电子文档安全管理产品自身安全功能要求等级划分

自身安全功能要求		第一级	第二级	第三级
组件安全	可信主机的自身保护功能	5.1.1	5.1.1	5.1.1
	防止非授权监控	5.1.2	5.1.2	5.1.2
	远程传输安全	5.1.3	5.1.3	5.1.3
管理员安全管理	标识与鉴别	5.2.1.1～5.2.1.4	5.2.1	5.2.1
	安全管理角色	—	5.2.2a)	5.2.2
	管理员管理	5.2.3a)	5.2.3	5.2.3
用户安全管理	授权用户唯一性标识	5.3.1	5.3.1	5.3.1
	用户管理	5.3.2	5.3.2	5.3.2
	用户分组管理	—	5.3.3	5.3.3
	用户角色管理	—	—	5.3.4
审计功能	审计日志生成	—	5.4.1a)、5.4.1b)	5.4.1
	审计日志存储	—	5.4.2a)	5.4.2
	审计日志管理	—	5.4.3a)、5.4.3b)	5.4.3

7.4 安全保证要求等级划分

电子文档安全管理产品的安全保证要求等级划分如表 3 所示。

表 3 电子文档安全管理产品安全保证要求等级划分

安全保证要求			第一级	第二级	第三级
配置管理	配置管理能力	版本号	6.1.1.1	6.1.1.1	6.1.1.1
		配置项	—	6.1.1.2	6.1.1.2
		授权控制	—	—	6.1.1.3

表 3（续）

安全保证要求			第一级	第二级	第三级
配置管理	配置管理覆盖		—	—	6.1.2
交付与运行	交付程序		—	—	6.2.1
	安装、生成和启动程序		6.2.2	6.2.2	6.2.2
开发	非形式化功能规范		6.3.1	6.3.1	6.3.1
	高层设计	描述性高层设计	—	6.3.2.1	6.3.2.1
		安全加强的高层设计	—	—	6.3.2.2
	非形式化对应性证实		6.3.3	6.3.3	6.3.3
指导性文档	管理员指南		6.4.1	6.4.1	6.4.1
	用户指南		6.4.2	6.4.2	6.4.2
生命周期支持			—	—	6.5
测试	覆盖	覆盖证据	—	6.6.1.1	6.6.1.1
		覆盖分析	—	—	6.6.1.2
	测试深度		—	—	6.6.2
	功能测试		—	6.6.3	6.6.3
	独立测试	一致性	6.6.4.1	6.6.4.1	6.6.4.1
		抽样	—	6.6.4.2	6.6.4.2
脆弱性分析保证	指南审查		—	—	6.7.1
	安全功能强度评估		—	6.7.2	6.7.2
	开发者脆弱性分析		—	6.7.3	6.7.3

中华人民共和国公共安全
行业标准
信息安全技术
电子文档安全管理产品安全技术要求
GA/T 989—2012
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100013)
北京市西城区三里河北街16号(100045)
网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946
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 1 字数 22 千字
2012年7月第一版 2012年7月第一次印刷
*
书号:155066·2-23785 定价 18.00元

打印日期:2012年7月23日 F009