ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1106—2013

信息安全技术
电子签章产品安全技术要求

Information security technology—
Security technical requirements for electronic signature products

2013-10-15 发布　　2013-10-15 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、深圳市艾泰克工程咨询监理有限公司、天津南大通用数据技术有限公司、山东得安信息技术有限公司。

本标准主要起草人：马海燕、李毅、张笑笑、顾健、俞优、赵婷、林华斌、陈文亭、王强。

信息安全技术
电子签章产品安全技术要求

1 范围

本标准规定了电子签章产品的安全功能要求、自身安全功能要求、安全保证要求及电子签章产品的等级划分要求。

本标准适用于电子签章产品的设计、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 信息系统 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

下列术语和定义适用于本文件。

3.1

电子签章 electronic signature

以数字证书为基础，以数字签名为核心技术，将数字签名与印章图片以及被签章对象绑定在一起，为签章对象提供完整性验证和真实性验证。它是数字签名可视化表现形式之一。

3.2

电子签章产品 electronic signature product

提供电子印章的制作和管理、签章、验章与审计功能的产品。一般由印章生成和管理服务器端和签章客户端组成。

3.3

电子印章 electronic stamp

物理印章在电子世界的表现形式，在电子世界中实现物理印章的功能，分为电子公章和个人私章等。

3.4

制章者 stamp maker

制作电子印章的机构或者个人。

3.5

印章所有者 stamp owner

拥有电子印章的机构或者个人。

3.6

签章对象　signing target

需要进行签章的目标对象，如：文档、表格、网页表单以及数据字段等。

3.7

签章　sign

持章者利用签章软件和电子印章对签章对象在电子世界模拟现实世界中的盖章过程。

3.8

签章结果　signature

签章者对签章对象签章后生成的数据信息。

3.9

签章结果文件　signed file

签章结果与被签章对象相关联形成的文件。

3.10

验章者　signature validater

对签章结果文件的真实性和完整性进行验证的机构或个人。

3.11

验章　validation signature

验章者对签章结果文件的真实性和完整性进行验证的过程。

4　安全功能要求

4.1　印章生成和管理

4.1.1　制章检查

产品应在生成印章前检查印章申请者的证书。对于检查不合格的证书，应禁止为其制章。检查项目包括：

a)　证书合法性检查，应是产品认可的证书签发机构签发的证书才被认为是合法证书；

b)　证书状态检查，如：证书是否被注销等；

c)　证书有效期检查。

4.1.2　印章生成

产品的印章生成功能应符合以下要求：

a)　生成的印章应包含印章图片；

b)　生成的印章应包含印章属性信息，如：印章所有者信息等；

c)　生成的印章应包含制章者的数字证书、数字签名，签名应满足以下要求：

1)　产品制章的签名算法应符合国家密码管理的相关规定；

2)　产品制章的签名运算应在制章者的私钥存储介质内进行。

4.1.3　印章备份与恢复

产品应具有印章数据备份和恢复功能。

4.1.4 印章状态管理

产品应具有印章状态管理功能，包括：

a） 对印章进行挂起，至少包括禁止使用此印章签章；

b） 对已经挂起的印章进行恢复，至少包括恢复使用此印章签章；

c） 对印章进行作废，作废后此印章将不能再签章。

4.1.5 印章授权管理

能够对印章的使用进行授权，个人私章能够自动授权给本人，单位章或者部门章能够授权给印章使用者。

4.1.6 印章审计管理

4.1.6.1 印章制作日志

对于印章制作应记录日志。日志应记录以下内容：

a） 日期、时间；

b） 制章者的唯一身份标识；

c） 印章的唯一标识；

d） 成功或者失败，如失败，记录失败原因。

4.1.6.2 签章、撤章日志

对于签章、撤章应记录日志。日志应记录以下内容：

a） 日期、时间；

b） IP 地址和 MAC 地址；

c） 签章者的数字证书序列号；

d） 印章的唯一标识；

e） 被签章文件名；

f） 被签章文件的摘要；

g） 成功或者失败，如失败，记录失败原因。

4.1.6.3 验章日志

对于验章失败，应记录日志。

4.2 签章和验章

4.2.1 证书检查

产品应在签章前检查签章者的证书。对于检查不合格的证书，应禁止其签章。检查项目包括：

a） 证书合法性检查，只有产品认可的证书签发机构签发的证书才被认为是合法证书；

b） 证书状态检查，如：证书是否被注销等；

c） 证书有效期检查。

4.2.2 权限检查

对于印章存储在用户处的情况，产品应在签章前检查当前用户是否具有当前印章的使用权限。对

于检查不合格的，应禁止其签章。

4.2.3 印章检查

对于印章存储在用户处的情况，产品应在签章前检查印章真实性、完整性。对于检查不合格的，应禁止其签章。

4.2.4 时间戳

产品应具有时间戳功能，由产品提供确切的时间标识。

4.2.5 离线签章

若产品提供离线签章功能，即：产品可授权在签章客户端不连接印章管理服务器端的情况下进行签章，则产品的离线签章功能应符合以下要求：

a) 限制离线签章的签章次数和有效期；

b) 在离线签章时对当前用户是否具有当前印章的使用权限进行检查，对于检查不合格的，应禁止其签章；

c) 在离线签章时对印章真实性、完整性进行检查，对于检查不合格的，应禁止其签章。

4.2.6 撤销签章

签章应能撤销，撤销签章应不破坏签章对象的完整性，应确保只有签章者本人能够撤销签章。

4.2.7 多次签章和撤销

应能使用同一个印章对签章对象进行多次签章和撤章。

4.2.8 会签

应能使用不同的印章对同一个签章对象进行签章和撤章。

4.2.9 透明签章

签章后，印章图片应显示在签章结果文件中，且不遮挡住图片背后的签章对象的内容，效果类似物理印章的盖章效果。

4.2.10 签章结果

产品应能对签章对象签章，签章结果应包含以下项目：

a) 印章信息，至少包括印章图片等；

b) 签章者数字证书；

c) 签章者对签章对象的数字签名，具体的要求见 4.2.11；

d) 签章者对印章信息的数字签名。

4.2.11 签章对象

4.2.11.1 特有格式的文档签章

如果产品支持对其特有格式的文档的签章，则产品应支持：

a) 对其特有格式文档的所有内容信息和所有格式信息的数字签名；

b） 将通用文档无差错地转化为其特有格式文档。

4.2.11.2 word 文档或“WPS 文字”文档签章

如果签章客户端支持对 word 文档或“WPS 文字”文档签章，则应支持对以下内容或格式信息的数字签名：

a） 主文本的文字内容、文字颜色、字号；

b） 表格的文字内容、颜色、字号；

c） 表格等对象的水平位置、垂直位置、行宽、列宽；

d） 除上述之外的其他所有内容和格式信息。

4.2.11.3 excel 文档或“WPS 表格”文档签章

如果签章客户端支持对 excel 文档或“WPS 表格”文档签章，则应至少支持对以下 excel 文档内容或格式信息的数字签名：

a） 表格的文字或算式内容、颜色、字号、所在行号、列号；

b） 表格的行宽、列宽；

c） 除上述之外的其他所有内容和格式信息。

4.2.11.4 pdf 文档签章

如果签章客户端支持对 pdf 文档签章，则应支持对 pdf 文档的所有内容或格式信息的数字签名。

4.2.11.5 AutoCAD 文档签章

如果签章客户端支持对 AutoCAD 文档签章，则应支持对 AutoCAD 文档的所有内容和格式信息的数字签名。

4.2.11.6 网页表单签章

如果签章客户端支持对网页表单的签章，则应支持对网页表单的所有指定域的内容和格式信息的数字签名。

4.2.12 签名算法

产品签章中使用的数字签名算法应符合国家密码管理局的相关规定。

4.2.13 签名运算空间

产品签章的签名运算应在签章者的私钥存储介质内进行。

4.2.14 验章

产品应能对签章结果文件验章。验章应符合以下要求：

a） 验证签章结果中的数字签名，如验证失败，应给出相应提示，并在印章图片上显示明显的标识；

b） 验证签章结果中的签章者证书的合法性，如验证失败，应给出相应提示，并在印章图片上显示明显的标识；

c） 验证签章结果的完整性。

4.2.15 自动验章

应能设置在签章结果文件打开时自动验证签章、显示结果。

5 自身安全功能要求

5.1 身份鉴别

身份鉴别应满足以下要求：

a） 对登录用户进行身份标识和鉴别；

b） 对同一用户采用两种或两种以上组合的鉴别技术实现用户身份鉴别；

c） 提供用户身份标识唯一功能，保证应用系统中不存在重复用户身份标识，身份鉴别信息不易被冒用；

d） 提供登录失败处理功能，可采取结束会话、限制非法登录次数和自动退出等措施；

5.2 访问控制

访问控制应满足以下要求：

a） 提供访问控制功能，依据安全策略控制用户对文件、数据库表等客体的访问；

b） 访问控制的覆盖范围应包括与资源访问相关的主体、客体及它们之间的操作；

c） 由授权主体配置访问控制策略，并严格限制默认账户的访问权限；

d） 授予不同账户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

5.3 审计功能

审计功能应满足以下要求：

a） 提供覆盖到每个用户的安全审计功能，对应用系统重要安全事件进行审计；

b） 保证无法单独中断审计进程；

c） 保证无法非授权地删除、修改或覆盖审计记录；

d） 审计记录的内容至少应包括事件的日期、时间、发起者信息、类型、描述和结果等；

e） 提供对审计记录数据进行统计、查询、分析及生成审计报表的功能。

5.4 剩余信息保护

剩余信息保护应满足以下要求：

a） 保证用户鉴别信息所在的存储空间被释放或再分配给其他用户前得到完全清除，无论这些信息是存放在硬盘上还是在内存中；

b） 保证产品的文件、目录和数据库记录等资源所在的存储空间被释放或重新分配给其他用户前得到完全清除。

5.5 通信完整性

应采用以下技术保证通信过程中数据的完整性：

a） 约定通信会话方式；

b） 校验码技术；

c） 采用密码。

5.6 通信保密性

通信保密性应满足以下要求：

a) 在通信双方建立连接之前，应利用密码技术进行会话初始化验证；
b) 对通信过程中的敏感信息字段进行加密；
c) 对通信过程中的整个报文或会话过程进行加密。

5.7 存储完整性

应能够检测到系统管理数据、鉴别信息和印章数据在存储过程中完整性受到破坏，并在检测到完整性错误时采取必要的恢复措施。

5.8 存储保密性

应采用加密或其他保护措施实现鉴别信息的存储保密性。

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。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) 用户可获取但应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，并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 测试覆盖

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。

深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

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 产品等级划分

7.1 概述

依据电子签章产品的开发、生产现状及实际应用情况，将电子签章产品安全功能要求、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

安全功能要求等级划分如表1所示。

表1 电子签章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
印章生成和管理	制章检查		—	4.1.1	4.1.1
	印章生成		4.1.2.a)	4.1.2 a)	4.1.2
	印章备份与恢复		—	—	4.1.3
	印章状态管理		—	4.1.4	4.1.4
印章生成和管理	印章授权管理		4.1.5	4.1.5	4.1.5
	印章审计管理	印章制作日志	—	4.1.6.1	4.1.6.1
		签章、撤章日志	—	4.1.6.2	4.1.6.2
		验章日志	—	—	4.1.6.3

表 1（续）

安全功能要求			第一级	第二级	第三级
签章和验章	证书检查		—	—	4.2.1
	权限检查		—	4.2.2	4.2.2
	印章检查		—	—	4.2.3
	时间戳		—	—	4.2.4
	离线签章		—	4.2.5a)	4.2.5
	撤销签章		—	4.2.6	4.2.6
	多次签章和撤销		—	—	4.2.7
	会签		—	—	4.2.8
	透明签章		4.2.9	4.2.9	4.2.9
	签章结果		4.2.10 a)～c)	4.2.10 a)～c)	4.2.10
	签名对象	特有格式的文档签章	4.2.11.1	4.2.11.1	4.2.11.1
		word 文档或“WPS 文字”文档签章	4.2.11.2 a)～c)	4.2.11.2 a)～c)	4.2.11.2
		excel 文档签章或“WPS 表格”文档签章	4.2.11.3 a)、b)	4.2.11.3 a)、b)	4.2.11.3
		pdf 文档签章	4.2.11.4	4.2.11.4	4.2.11.4
		AutoCAD 文档签章	4.2.11.5	4.2.11.5	4.2.11.5
		网页表单签章	4.2.11.6	4.2.11.6	4.2.11.6
	签名算法		4.2.12	4.2.13	4.2.13
	签名运算空间		4.2.13	4.2.13	4.2.13
	验章		4.2.14 a)、b)	4.2.14 a)、b)	4.2.14
	自动验章		—	—	4.2.15

7.3 自身安全功能要求等级划分

自身安全功能要求等级划分如表 2 所示。

表 2 电子签章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
身份鉴别	5.1 a)～c)	5.1 a)～c)	5.1
访问控制	5.2 a)～c)	5.2	5.2
审计功能	—	5.3 a)～d)	5.3
剩余信息保护	5.4	5.4	5.4
通信完整性	—	5.5 a)、b)	5.5
通信保密性	—	5.6 a)、b)	5.6
存储完整性	—	—	5.7
存储保密性	—	—	5.8

7.4 安全保证要求等级划分

安全保证要求等级划分如表 3 所示。

表 3 电子签章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
	配置管理覆盖		—	—	6.1.2
交付与运行	交付程序		—	6.2.1	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	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