



中华人民共和国国家标准

GB/T 25065—2010

信息安全技术 公钥基础设施 签名生成应用程序的安全要求

Information security technology—Public key infrastructure—
Security requirements for signature creation applications

2010-09-02 发布

2011-02-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会 发布

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 公钥基础设施
签名生成应用程序的安全要求

GB/T 25065—2010

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

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 2.75 字数 77 千字

2010年12月第一版 2010年12月第一次印刷

*

书号: 155066·1-40583

如有印装差错 由本社发行中心调换

版权专有 侵权必究

举报电话:(010)68533533

目 次

前言	V
1 范围	1
2 规范性引用文件	1
3 术语和定义	1
4 缩略语	3
5 签名生成的功能模型	3
5.1 签名生成的目标	3
5.2 功能模型	3
5.3 签名生成应用程序	5
5.4 安全签名生成设备	6
5.5 签名生成应用程序实例	7
5.6 签名生成系统的控制和拥有	7
6 签名数据对象信息模型	7
6.1 签名人文件	8
6.2 签名属性	8
6.3 待签数据	9
6.4 格式化的待签数据	9
6.5 待签数据表示	9
6.6 可靠电子签名	9
6.7 签名数据对象	9
6.8 签名人鉴别数据	9
7 SCA 的总体安全要求	10
7.1 基本要求	10
7.2 可信路径	10
7.3 分布式签名生成应用程序的要求	11
7.4 对不可信进程和通信端口的要求	11
7.5 签名数据对象的事后签名验证	11
7.6 对待签数据的安全要求	11
8 SD 表示组件	12
8.1 功能	12
8.2 分类	12
8.3 数据内容类型的要求	12
8.4 SD 无歧义性要求	13
8.5 对显示不敏感的 SD 的安全要求	14
8.6 对隐藏文本和活动代码的要求	14
9 签名属性显示组件	14
10 签名人交互组件	15
10.1 用户界面高层原理	15

- 10.2 签名调用 15
- 10.3 签名进程超时休止 16
- 10.4 签名人控制功能 16
- 10.5 签名人使用特征的获得 16
- 10.6 用户界面 16
- 11 签名人鉴别组件 17
 - 11.1 总体要求 17
 - 11.2 获得签名人鉴别数据 17
 - 11.3 基于知识的签名人鉴别 17
 - 11.4 基于生物特征的签名人鉴别 17
 - 11.5 对错误的签名人鉴别数据的处理 18
 - 11.6 签名人鉴别数据的变更和计数器重置 18
 - 11.7 签名人鉴别数据用户界面 18
 - 11.8 签名人鉴别组件的安全要求 18
- 12 DTBS 格式化组件 20
 - 12.1 DTBS 格式化组件的功能 20
 - 12.2 对 DTBS 格式化组件的安全要求 20
- 13 数据杂凑/散列组件 20
 - 13.1 数据杂凑/散列组件的功能 20
 - 13.2 DTBSR 的产生组件的输出结果 20
 - 13.3 电子签名输入的格式化 21
 - 13.4 对数据杂凑/散列组件的安全要求 21
- 14 SSCD/SCA 通信组件 22
 - 14.1 交互序列 22
 - 14.2 建立物理通信连接 23
 - 14.3 SSCD 令牌信息的读取 23
 - 14.4 在多应用平台上 SSCD 功能的选择 24
 - 14.5 证书的获取 24
 - 14.6 电子签名制作数据的选择 24
 - 14.7 签名人鉴别的执行 25
 - 14.8 数字签名的计算 25
 - 14.9 签名日志的记录 25
 - 14.10 对 SSCD/SCA 通信组件的安全要求 25
- 15 SSCD/SCA 鉴别组件 25
 - 15.1 SCA 与 SSCD 之间的鉴别 25
 - 15.2 对 SSCD/SCA 鉴别组件的安全要求 26
- 16 SD 合成组件 26
- 17 SDO 合成组件 26
- 18 输入/输出的外部接口 27
 - 18.1 SCA 面临的风险 27
 - 18.2 证书的导入 27
 - 18.3 SD 和签名属性的导入 27
 - 18.4 SCA 组件的下载 27

18.5 对输入控制的安全要求	27
附录 A (资料性附录) 签名数据对象通用指导	28
附录 B (资料性附录) 用户接口实现的指导	30
附录 C (资料性附录) 签名日志组件(SLC)	35
参考文献	36

前 言

本标准凡涉及密码算法的相关内容,按国家有关法规实施。

本标准中引用的 RSA 和 SHA-1 密码算法为举例性说明,具体使用时均须采用国家密码管理机构批准的相应算法。

本标准参考 EESSI 标准《CWA14170-签名生成应用程序的安全要求》。

本标准中的附录 A、附录 B、附录 C 是资料性附录。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:北京天威诚信电子商务服务有限公司、中国电子技术标准化研究所、北京邮电大学。

本标准主要起草人:刘海龙、唐志红、宋美娜、鄂海红、王延鸣、张海松、杨真、许蕾、邵哲。

信息安全技术 公钥基础设施 签名生成应用程序的安全要求

1 范围

本标准规定了产生可靠电子签名的签名生成应用程序(SCA)的安全要求,内容包括:定义一种签名生成环境的模型和签名生成应用程序的功能模型;规定适用于功能模型中所有功能模块的总体要求;规定签名生成应用程序中每个功能模块的安全要求,除了 SSCD。

本标准适用于所有用于生成可靠电子签名的签名生成应用程序。

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 25064—2010 信息安全技术 公钥基础设施 电子签名格式规范

3 术语和定义

下列术语和定义适用于本标准。

3.1

可靠电子签名 reliable electronic signature

能符合以下条件的电子签名:电子签名制作数据用于电子签名时,属于电子签名人专有;签署时电子签名制作数据仅由电子签名人控制;签署后对电子签名的任何改动能够被发现;签署后对数据电文内容和形式的任何改动能够被发现。

3.2

证书标识符 certificate identifier

证书的一个明确标识符。

3.3

电子认证服务提供者 certification-service-provider

一个实体,或者是法人或自然人,颁发证书或提供与电子签名相关的其他服务。

3.4

加密设备 cryptographic token

能够执行加密操作的个人安全设备。签名生成设备即是一种加密设备。

3.5

待签数据 data to be signed

所要签署的完整电子数据。

3.6

格式化的待签数据 data to be signed formatted

已经被格式化的 DTBS 组成部件,并且按照签名人所选择 SDO 类型的要求正确排序。

3.7

DTBS 表示 DTBS-representation

由签名生成应用发送给签名生成设备的、需要被签署的数据。