ICS 35.240.40
L 80

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

目　　次

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。