ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25064—2010

信息安全技术　公钥基础设施 电子签名格式规范

Information security technology—Public key infrastructure—Electronic signature formats specification

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

目　　次

前　言

本标准的附录A和附录B为规范性附录。

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:中国科学院软件研究所信息安全国家重点实验室、信息安全共性技术国家工程研究中心。

本标准主要起草人:张凡、冯登国、庄涌、张立武、路晓明、杨婧。

引　言

电子商务作为跨越本地、广域、全球网络的新型商务模式，可信对于其成功和连续进行至关重要。以电子方式进行商务活动的公司必须有适合的安全控制机制来保护他们的交易并确保交易方的安全，而电子签名对于保护信息和提供电子商务中的信任是一项重要的安全措施。

本标准主要参考了 ETSI TS 101 733 V1.2.2 (2000-12)，并以我国电子签名法为纲，针对各种类型的电子签名，可以应用于各种业务，包括个人与公司、公司与公司、个人与政府。本标准独立于应用环境，可以应用在智能卡、GSM SIM 卡、电子签名的特殊应用等各种环境中。根据本标准生成的电子签名并满足《中华人民共和国电子签名法》第十三条规定，即认为是可靠的电子签名。

本标准凡涉及密码算法相关内容，按国家密码管理部门相关规定执行。

本标准例子中提及的密码算法如 SHA-1 算法均为举例性说明，具体使用时均须采用国家密码管理部门批准的相应算法。

信息安全技术　公钥基础设施
电子签名格式规范

1　范围

本标准针对基于公钥密码学生成的数字签名类型的电子签名，定义了电子签名与验证的主要参与方、电子签名的类型、验证和仲裁要求。本标准还规范了电子签名的数据格式，包括基本数据格式、验证数据格式、签名策略格式等。

本标准适用于电子签名产品的设计和实现，同时相关产品的测试、评估和采购亦可参照使用。

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 16264.8—2005　信息技术　开放系统互连　目录　第8部分：公钥和属性证书框架（ISO/IEC 9594-8：2001，IDT）

GB/T 16262.1—2006　信息技术　抽象语法记法一（ASN.1）　第1部分：基本记法规范（ISO/IEC 8824-1：2002，IDT）

GB/T 19713—2005　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 20520—2006　信息安全技术　公钥基础设施　时间戳规范

RFC2630　加密消息语法

RFC2634　S/MIME的增强安全服务

3　术语和定义

下列术语和定义适用于本标准。

3.1

签名者　signer

电子签名人，创建电子签名的实体。

3.2

验证者　verifier

电子签名依赖方，对电子签名进行合法性验证的实体。

3.3

仲裁者　arbitrator

当数字签名的有效性发生争议时，对签名者和验证者之间的争议进行仲裁的实体。

3.4

可信服务提供者　trusted service provider

帮助签名者和验证者建立信任关系的一个或多个实体。

3.5

时间戳　time stamp

使用数字签名技术产生的数据，签名的对象包括了原始文件信息、签名参数、签名时间等信息。时