ICS 35.040
L 80

中华人民共和国国家标准

GB/T 35285—2017

信息安全技术　公钥基础设施 基于数字证书的可靠电子签名 生成及验证技术要求

Information security technology—Public key infrastructure—Technical requirements for digital certificate based reliable electronic signature creation and verification

2017-12-29 发布　　2018-07-01 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 …… Ⅰ
引言 …… Ⅱ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 2
5　可靠电子签名生成及验证系统架构 …… 3
5.1　可靠电子签名生成及验证逻辑框架 …… 3
5.2　可靠电子签名生成及验证涉及的对象 …… 3
6　电子认证服务提供者的要求 …… 4
6.1　电子认证服务提供者的基本条件 …… 4
6.2　电子认证服务提供者提供的服务及安全要求 …… 4
7　电子签名人身份的要求 …… 5
8　电子签名相关数据的要求 …… 5
8.1　待签数据的要求 …… 5
8.2　电子签名数据格式的要求 …… 6
9　签名生成模块的要求 …… 6
9.1　功能要求 …… 6
9.2　安全要求 …… 6
10　电子签名生成过程与应用程序要求 …… 7
10.1　电子签名生成过程要求 …… 7
10.2　签名生成应用程序要求 …… 8
11　电子签名验证过程与应用程序要求 …… 9
11.1　电子签名验证过程要求 …… 9
11.2　签名验证应用程序要求 …… 9
参考文献 …… 10

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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:中国电子信息产业发展研究院、北京数字认证股份有限公司、上海格尔软件股份有限公司、标新科技(北京)有限公司、中标信安科技(北京)有限公司、北京证联信通科技发展有限公司、重庆邮电大学。

本标准主要起草人:刘权、陈月华、许亚倩、林雪焰、傅大鹏、王闯、叶枫、刘东华、段勐、马圣东、黄永洪。

引　言

随着电子政务、电子商务等网络应用的快速发展，信息失窃、网络欺诈等现象日益突出，电子签名作为确认网络主体及行为、认定法律责任和保障合法权益的重要手段，应用日趋广泛。《中华人民共和国电子签名法》没有规定必须采用某种特定的技术，但以目前国际上比较公认的、技术成熟的技术看，主要是基于数字证书的电子签名技术。

虽然《中华人民共和国电子签名法》确立了可靠电子签名的法律效力，但如何从技术上实现可靠电子签名以及如何验证电子签名是可靠的等问题，仍没有得到很好的解决。为贯彻落实《中华人民共和国电子签名法》，促进可靠电子签名的应用普及，有必要对可靠电子签名的生成及验证技术规范进行研究和制定。本标准凡涉及电子签名技术相关内容，均指基于数字证书的电子签名技术。在本标准实施过程中，涉及密码技术的具体应用时，按照国家密码主管部门发布的有关规定和技术规范执行。

信息安全技术　公钥基础设施
基于数字证书的可靠电子签名
生成及验证技术要求

1　范围

本标准规定了基于数字证书的可靠电子签名生成及验证过程的技术要求，包括电子认证服务提供者、电子签名人身份、电子签名相关数据、签名生成模块、电子签名生成过程与应用程序、电子签名验证过程与应用程序等要求。

本标准适用于基于数字证书的可靠电子签名相关系统、应用的开发，以及相关产品、服务标准的制定。

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 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

GB/T 25064—2010　信息安全技术　公钥基础设施　电子签名格式规范

GB/T 25069—2010　信息安全技术　术语

3　术语和定义

GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

电子签名人　electronic signer

持有电子签名制作数据并以本人身份或者以其所代表的人的名义实施电子签名的人，也称为签名方。

3.2

电子签名　electronic signature

数据电文中以电子形式所含、所附用于识别电子签名人身份并表明电子签名人认可其中内容的数据。

3.3

电子签名制作数据　electronic signature creation data

在电子签名制作过程中使用的、将电子签名与电子签名人可靠地联系起来的字符、编码等数据。在基于公钥技术实现的电子签名中，电子签名制作数据也称为私钥。

3.4

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；签名时电