ICS 35.040
L 80

中华人民共和国国家标准

GB/T 31503—2015

信息安全技术
电子文档加密与签名消息语法

Information security technology—
Encryption and signature message syntax for electronic document

2015-05-15 发布　　2016-01-01 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:中国科学院数据与通信保护研究教育中心、北京数字认证股份有限公司、上海普华诚信信息技术有限公司、赞嘉电子科技有限公司。

本标准主要起草人:向继、汪婧、王雷、荆继武、高能、林璟锵、管乐、马存庆、查达仁、詹榜华、梁佐泉、张嘉纯。

引　言

本标准主要参考 IETF(互联网工程特别工作组)RFC 5652 文件制定。

本标准规定了用于电子文档密码保护的封装语法。它支持数字签名和加密。该语法允许多重封装,一个封装信封可以嵌套在另一个封装信封之内,同样,一方可以对以前封装过的数据再进行数字签名。它也允许任意属性,如签名时间,同消息内容一起签名,并且提供其他属性如联合签名,同签名关联在一起。

本标准描述的电子文档加密与签名消息语法支持各种基于证书的密钥管理架构。该语法使用抽象语法记法 ASN.1,并采用 BER 编码生成值。这些值通常表示成字节串的形式。虽然很多系统都能够可靠地传输字节串,但仍有很多电子邮件系统不行。本标准不提供字节串编码机制以保证这种环境下的可靠传输。

信息安全技术
电子文档加密与签名消息语法

1 范围

本标准规定了电子文档加密与签名消息语法，此语法可用于对任意消息内容进行数字签名、摘要、鉴别或加密。

本标准适用于电子商务和电子政务中电子文档加密与签名消息的产生、处理以及验证。

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 16262.1—2006 信息技术 抽象语法记法—(ASN.1) 第1部分：基本记法规范

GB/T 16263.1—2006 信息技术 ASN.1编码规则 第1部分：基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范

GB/T 16264.2—2008 信息技术 开放系统互连 目录 第2部分：模型

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

GB/T 19714—2005 信息技术 安全技术 公钥基础设施 证书管理协议

GB/T 20518—2006 信息安全技术 公钥基础设施 数字证书格式

RFC 3281 用于授权的因特网属性证书框架(An Internet Attribute Certificate Profile for Authorization)

RFC 5280 因特网X.509公钥基础设施证书和证书撤销列表轮廓(Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile)

3 术语和定义

GB/T 19714—2005、GB/T 20518—2006界定的以及下列术语和定义适用于本文件。

3.1

算法标识符 algorithm identifier

通过对象标识符标识算法的类型。

3.2

属性 attribute

包括属性类型以及一个或多个属性值，属性类型由对象标识符指定。

4 缩略语

下列缩略语适用于本文件。

ASN.1：抽象语法记法—(Abstract Syntax Notation one)

BER：基本编码规则 (Basic Encoding Rules)