ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25061—2020
代替 GB/T 25061—2010

信息安全技术
XML 数字签名语法与处理规范

Information security technology—
XML digital signature syntax and processing specification

2020-11-19 发布　　2021-06-01 实施

国家市场监督管理总局
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。

本标准代替 GB/T 25061—2010《信息安全技术　公钥基础设施 XML 数字签名语法与处理规范》，与 GB/T 25061—2010 相比，主要技术变化如下：

——增加了新的引用文件(见第 2 章)；

——在 KeyInfo 中，增加了 SM2KeyValue 类型定义，表示 SM2 椭圆曲线密码算法密钥值(见 6.5.3.3)；

——在 KeyInfo 元素中，增加了 DEREncodedKeyValue 和 KeyInfoReference 子元素，并给出模式定义(见 6.5.6 和 6.5.7)；

——增加了 xmldsig11-schema.xsd 和 xmldsig1-schema.xsd 的定义(见附录 C 中 C.2 和 C.3)；

——增加了密码杂凑算法 SM3，消息鉴别算法 HMAC-SM3，签名算法 SM2-SM3 的定义(见附录 D 中 D.3.2、D.4.3 和 D.5.3)；

——增加了 XML 规范化 1.1 算法和独占 XML 规范化 1.0 算法(见附录 D 中 D.6.3 和 D.6.4)。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

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：北京信安世纪科技股份有限公司、格尔软件股份有限公司、数安时代科技股份有限公司、国家密码管理局商用密码检测中心。

本标准主要起草人：汪宗斌、刘婷、郑强、张永强、吕春梅、焦靖伟、史晓峰。

本标准所代替标准的历次版本发布情况为：

——GB/T 25061—2010。

信息安全技术
XML 数字签名语法与处理规范

1 范围

本标准规定了创建和表示 XML 数字签名的处理规则、签名语法、附加的签名语法和证实方法。

本标准适用于制作和处理 XML 数字签名的应用程序、系统或服务。

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 1988 信息技术 信息交换用七位编码字符集

GB/T 13000 信息技术 通用多八位编码字符集(UCS)

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 18793—2002 信息技术 可扩展置标语言(XML)1.0

GB/T 20518—2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 35276—2017 信息安全技术 SM2 密码算法使用规范

RFC 2045 基于多用途互联网邮件扩展 第 1 部分：互联网消息体格式(Multipurpose Internet Mail Extensions(MIME) Part One: Format of Internet Message Bodies)

RFC 3279 互联网 X.509 公钥基础设施的算法和标识符 证书和证书撤销列表轮廓[Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile]

RFC 3986 统一资源标识符(URI)：通用语法[Uniform Resource Identifier (URI): Generic Syntax]

RFC 4514 轻型目录访问协议(LDAP)：甄别名的字符串表示[Lightweight Directory Access Protocol (LDAP): String Representation of Distinguished Names]

RFC 5480 椭圆曲线密码主体公钥信息(Elliptic Curve Cryptography Subject Public Key Information)

3 术语、定义和缩略语

3.1 术语和定义

GB/T 18793—2002 界定的以及下列术语和定义适用于本文件。

3.1.1

分离签名 detached signature

签名于 Signature 元素以外的内容上，签名和数据对象位于不同 XML 文档中的 XML 签名文档的组织形式。