ICS 35.040
L 80

中华人民共和国国家标准

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

Information security technology—Public Key Infrastructure—XML digital signature syntax and processing 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是规范性附录，附录C和附录D是资料性附录。

本标准主要参照Internet工程任务组(IETF)的RFC 3275文件制定。

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：北京信安世纪科技有限公司、中国电子技术标准化研究所。

本标准起草人：汪宗斌、张萌、黄勇、周鹏、王延鸣。

引　言

XML 是一种信息描述的置标语言，用于数据对象交换。它已经广泛地应用在电子商务、电子政务等应用之中，成为数据交换当中数据描述的基础格式，并且仍在不断发展当中。基于 XML 格式的数字签名是 XML 在安全领域的一种新的应用，与传统的 PKCS#7 数字签名相比，能够更好地与 XML 应用结合。

本标准凡涉及密码算法相关内容，标准文本中引用的 RSA 和 SHA-1 等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局批准的相应算法。

信息安全技术　公钥基础设施
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 数字签名的语法和处理规则。XML 数字签名为任何类型的数据提供了完整性、消息鉴别和签名者鉴别服务。

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 1988　信息技术　信息交换用七位编码字符集(GB/T 1988—1998，eqv ISO/IEC 646-1991)

GB 13000.1　信息技术　通用多八位编码字符集(UCS)　第一部分：体系结构和基本多文种平面(GB 13000.1—1993，idt ISO/IEC10646-1：1993)

GB/T 16264.8　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 16264.8—2005，ISO/IEC 9594-8：2001，IDT)

GB/T 18793—2002　信息技术　可扩展置标语言(XML)1.0 (W3C RFC-xml：1998，NEQ)

RFC 2253　轻型目录访问协议(v3)：甄别名的 UTF-8 字符串表示

RFC2396　统一资源标识符(URI)：通用语法

RFC2732　URL 中 IPv6 地址文字格式

3　术语、定义和缩略语

3.1　术语和定义

下列术语和定义适用于本标准。

3.1.1

分离签名　detached signature

签名于 Signature 元素以外的内容上，通过 URI 或者变换来进行标识，和它所签署的内容是分开的。即签名和数据对象位于不同 XML 文档中。适用于签名与数据分离的情形(即不同的 XML 文档)，或者相同的 XML 文件包括了签名和数据对象，但签名和数据对象是兄弟元素的情形。

3.1.2

封内签名　enveloping signature

签名于 Signature 元素中的 Object 元素之上，以 Signature 为父元素，将原始文档包含在 Signature 中的 XML 签名文档的组织形式。即通过对封装了的对象的签名进行封装。

3.1.3

封皮签名　enveloped signature

签名于整个 XML 内容之上，然后将 Signature 作为子元素插入到原始文档中，组织成 XML 签名文档格式。即将签名封装到 XML 对象中，封皮签名在计算 SignatureValue 时不包含其自身。