ICS 35.040
L 80

中华人民共和国国家标准

GB/T 25060—2010

信息安全技术　公钥基础设施 X.509数字证书应用接口规范

Information security techniques—Public Key Infrastructure—Interface specification of X.509 digital certificates application

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

本标准凡涉及密码算法相关内容，按国家有关法规实施。

本标准的附录A为规范性附录。

本标准由全国信息安全标准化技术委员会(TC 260)提出并归口。

本标准起草单位：长春吉大正元信息技术股份有限公司。

本标准主要起草人：李伟平、何长龙、刘勇、付敏。

引　言

基于PKI技术体系的电子签名和电子认证为电子政务和电子商务的开展提供了技术支持，特别是《中华人民共和国电子签名法》的颁布为基于电子签名的应用提供了法律依据。但是，由于各厂商对数字证书应用需求理解的差异性及实践经验不足，数字证书应用API实现存在很大的随意性，以及相关标准规范的缺乏，导致各厂家同类产品间差别大，给基于数字证书应用、应用系统集成和数字证书管理及推广带来极大困难。

对基于数字证书应用需求进行研究、总结，统一规划、编制基于PKI技术体系的数字证书应用接口规范，有利于数字证书应用产品提供商缩短产品研发周期，减少研发和支持成本；有利于应用开发商和服务商摆脱特定CA提供的接口而在规范的数字证书应用接口上进行数字证书应用的开发，减少针对开发的设计、实现和测试，使其能够专注于应用产品功能；有利于降低数字证书应用的复杂度，并便于用户对数字证书的使用。

本标准基于《公钥密码基础设施应用技术体系　通用密码服务接口规范》，进行了适当剪裁，针对数字证书应用进行了规范，可用于指导数字证书认证系统中数字证书应用产品的研制和开发。

本标准在编写过程中得到了商用密码基础设施专项工作组的指导。

信息安全技术　公钥基础设施
X.509数字证书应用接口规范

1　范围

本标准定义了数字证书应用标识及一组证书应用接口。

本标准适用于基于数字证书的安全中间件的设计和实现，对基于数字证书的安全功能的研制、开发、测试亦可参照使用。

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 20518—2006　信息安全技术　公钥基础设施　数字证书格式

PKCS#7 V1.5：加密消息语法标准

3　术语和定义

下列术语和定义适用于本标准。

3.1

数字证书　digital certificate

由认证权威数字签名的包含公开密钥拥有者信息、公开密钥、签发者信息、有效期以及一些扩展信息的数字文件。

3.2

证书撤销列表　certificate revocation list

标记一系列不再被证书发布者所信任的证书的签名列表。

3.3

数字信封　digital envelope

附加到消息中的数据，它允许消息的预期接收方验证该消息内容的完整性。

4　缩略语

下列缩略语适用于本标准。

CA	证书认证机构	(Certificate Authority)
CRL	证书撤销列表	(Certificate Revocation List)
DER	可区分编码规则	(Distinguished Encoding Rules)
PKCS#1	RSA加密标准	(RSA Cryptography Standard)
PKCS#7	加密消息的语法标准	(Cryptographic Message Syntax Standard)
PKI	公钥基础设施	(Public Key Infrastructure)
OID	对象标识符	(Object Identifier)