ICS 35.100.70
L 79

中华人民共和国国家标准

GB/T 19771—2005

信息技术　安全技术　公钥基础设施 PKI组件最小互操作规范

Information technology—Security technology—Public key infrastructure —Minimum interoperability specification for PKI components

2005-05-25 发布　　2005-12-01 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

本标准是在参考美国国家标准与技术研究院(NIST)提出的《公钥基础设施 PKI 组件最小互操作规范》第二版内容的基础上修改而成,同时本标准还参照了包括证书管理策略(CMP)、证书请求消息格式(CRMF)、FIPS 许可的密码算法和 X9 密码算法等相关的规范。

本标准凡涉及密码算法相关内容,按国家有关法规实施。

本标准中引用的 SHA-1、RSA、SHA1-MAC、SHA1-HMAC 、DES-MAC、tDEA 密码算法均为举例性说明,具体使用时均须采用国家商用密码管理委员会批准的相应算法。

本标准的附录 A、附录 B、附录 C、附录 D 为规范性附录。

本标准由中华人民共和国信息产业部提出。

本标准由全国信息安全标准化技术委员会(TC260)归口。

本标准起草单位:信息安全国家重点实验室、中国电子技术标准化研究所。

本标准主要起草人:冯登国、吴志刚、荆继武、高 能、向 继、张 凯、周瑞辉、徐 佳、林璟锵、曹 政、余婧、廖洪銮、李 丹、罗锋盈、陈 星。

引　言

数字签名证书在政府服务商业和法律程序中代替手写签名，并且允许以前没有联系的双方可靠地鉴别对方以进行商业事务。加密证书提供了加密传输和加密算法的应用，来建立或保护对称密钥以提供机密性。这样的一个公钥基础设施（PKI）系统和它相应的证书，也许远远超出了一些应用的实际需要，对那些特别的应用要求来说改进的证书和协议更合适。

信息技术　安全技术　公钥基础设施 PKI组件最小互操作规范

1　范围

本标准支持大规模公钥基础设施(PKI负责发布、撤销和管理用于数字签名及密钥管理的公钥证书)的互操作性。本标准为不同的PKI开发者所开发的组件产品提供了基本的互操作性参考。

本标准的内容涉及：

- 公钥证书的产生、更新和撤销；
- 签名的产生和验证；
- 证书和证书认证路径验证。

本标准主要包括了对证书、证书撤销列表(CRL)扩展和一套事务的描述。这些事务包括证书申请、证书更新、证书撤销以及从资料库检索证书和CRL。

本标准主要以最终用户的角度来看待PKI的互操作性，即怎样申请和获得一个证书；怎样签署文档；怎样检索他人的证书；怎样验证签名。就像下面所提及的，PKI的“内部”操作规范还没有达到足够成熟，因此它们没有被详细规定。

在本标准中PKI被分成五个组件：

- 颁发和撤销证书的证书认证机构(CAs)；
- 确保公钥和证书持有者的身份以及别的属性之间绑定的注册机构(RAs)；
- 获得证书和签署文档的证书持有者；
- 验证签名并且执行密钥管理协议以及验证证书认证路径的客户；
- 存储并提供对证书和CRL查询的资料库。

许多实体在功能上既是证书持有者又是客户。CAs和RAs也是如此。终端实体证书持有者通常也是客户。当然，也有一些客户并不是证书持有者。

资料库不必是证书持有者和客户。本标准仅仅涉及资料库协议的一部分，那就是客户要求从资料库中获得证书和CRL的信息。

本标准将轻型目录访问协议(LDAP)版本2作为用户访问资料库的传输手段，因为它是被广泛接受和采用的方法。例如，这种选择既不强调CA用来更新资料库的标准化协议，也不强调资料库之间互相映射的协议，尽管它们都是需要的。前者可以具体情况具体分析以解决CA和资料库之间的协议，后者也许并不必要。

在通常的证书状态确认(本标准遵循的)中，资料库不是可信实体，CA对CRL的签名更可靠。在线证书状态实时确认机制要求资料库是可信实体，而且它们也能让客户相信他们的身份。这样的证书状态确认协议超出了本标准的范围，但是在一些应用中可能需要实时证书状态确认，所以在以后的修订版中可能会解决这个问题。

本标准中没有提供让资料库验证使用者的协议，该协议是资料库记费应用的前提。虽然这可能是资料库重要的商用模式，但目前人们对该模式的看法还没有达到一致，也没有统一的支撑协议。在以后的修订版中可能会解决这个问题。

在一些情况下，带外事务也是本标准中事务的一部分。带外事务的形式和内容超出了本标准的范围。

本标准假定CA、RA和证书持有者是物理上分离的。如果这些实体在物理上是在一起的话，那么