ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29241—2012

信息安全技术　公钥基础设施 PKI互操作性评估准则

Information security technology—Public key infrastructure—PKI interoperability evaluation criteria

2012-12-31 发布　　2013-06-01 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 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、赞嘉电子科技(北京)有限公司。

本标准主要起草人:荆继武、马存庆、林璟锵、查达仁、吴晶晶、张帆、王平建。

引　言

PKI 系统作为普适性的安全基础设施，同时为各种不同的应用提供安全服务。通过 PKI 提供的安全服务信息，PKI 应用可以获得真实性、保密性、完整性、非否认等安全服务。

由于 PKI 系统的设计建设和运行维护所依据的标准和规范具有较大的灵活性和可选自由度，应用从 PKI 系统获得的服务数据也就具有一定的不确定性。证书私有扩展大量使用和证书策略意义不明确、撤销状态信息不全面等问题，都会影响安全服务的使用，甚至导致应用无法获得安全服务。上述问题，对于跨域的 PKI 事务尤为突出。由于跨域的 PKI 应用和 PKI 系统通常由不同的厂商或设计开发人员实现，双方对于各种服务数据的理解和使用不一致更加明显，导致二者之间难以互操作，难以获取安全服务。

当 PKI 系统进行互联互通时，就必须考虑 PKI 系统为跨域 PKI 应用提供安全服务信息的水平，也就是 PKI 系统与 PKI 应用之间的互操作问题。为更多的跨域应用提供全面的安全服务信息，是 PKI 系统进行互操作能力优化和改进的目标。如果 PKI 系统仅限于为特定的少数 PKI 应用提供服务，那么该 PKI 系统则难以在互联互通中发挥效用。作为一种安全基础设施，PKI 系统应该面向各种应用，采取有效的办法提高互操作能力，为网络通信做好全面的安全基础。另一方面，用户会希望自己的 PKI 应用能够与更多的 PKI 系统互操作，有能力从不同的电子认证服务机构获得安全服务。

本标准考虑了 PKI 安全服务相关的各种信息及其性能。PKI 系统提供安全服务的方式是生成各种证书的相关信息，包括：证书、证书撤销状态信息、证书策略和认证业务声明等。PKI 应用就是利用上述信息获得安全服务。安全服务信息的格式是否正确设置、内容是否明确表达、功能体现是否完善、操作过程是否按标准化执行、信息来源是否可靠等问题，都会影响安全服务的提供。

本标准分别从 PKI 系统和 PKI 应用 2 个方面，提出了分等级的互操作性评估准则。高等级的 PKI 系统，能够为更多的 PKI 应用提供更全面可靠的安全服务。高等级的 PKI 应用，能够从更多的 PKI 系统中获取更全面的安全服务。

本标准通过分等级的互操作评估，为 PKI 系统和 PKI 应用都指出了改进的方向，将促进建设和开发具有全面互操作能力的 PKI 系统和应用，从而为 PKI 系统的全面互联互通，为最终形成统一的认证体系，奠定坚实的基础。

信息安全技术　公钥基础设施
PKI互操作性评估准则

1　范围

本标准规定了PKI系统和PKI应用的五个互操作能力等级，完成了分等级的PKI互操作性评估准则，为PKI系统和PKI应用提供了互操作能力等级评估的依据。

本标准适用于需要进行跨域互操作的PKI系统和PKI应用，可用于PKI系统和PKI应用的设计、开发、制造、采购、测试、评估、使用等过程。

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 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 19713—2005　信息技术　安全技术　公钥基础设施　在线证书状态协议

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GM/T 0003—2012　SM2椭圆曲线公钥密码算法

GM/T 0004—2012　SM3密码杂凑算法

RFC 3647　因特网X.509公钥基础设施：证书策略和认证业务框架(Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework)

RFC 3709　因特网X.509公钥基础设施：X.509证书中的徽标(Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates)

RFC 3779　用于IP地址和AS标识符的X.509证书扩展(X.509 Extensions for IP Addresses and AS Identifiers)

RFC 4059　因特网X.509公钥基础设施：担保信息证书扩展(Internet X.509 Public Key Infrastructure: Warranty Certificate Extension)

RFC 4334　支持点对点协议(PPP)和无线局域网(WLAN)鉴别的证书扩展和属性[Certificate Extensions and Attributes Supporting Authentication in Point-to-Point Protocol (PPP) and Wireless Local Area Networks (WLAN)]

RFC 4387　因特网X.509公钥基础设施操作协议：通过HTTP访问证书存储(Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP)

RFC 4523　用于X.509证书的轻量级目录访问协议(LDAP)模式定义(Lightweight Directory Access Protocol(LDAP) Schema Definitions for X.509 Certificates)

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

3　术语和定义

GB/T 16264.8—2005界定的以及下列术语和定义适用于本文件。