ICS 35.040
L 80

中华人民共和国国家标准

GB/T 29243—2012

信息安全技术　数字证书代理认证路径构造和代理验证规范

Information security technology—Specifications of delegated certification path construction and delegated validation for digital certificate

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 给出的规则起草。

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。

本标准主要起草人:夏鲁宁、王琼霄、荆继武、林璟锵、向继。

本标准为首次制定。

引　言

随着《中华人民共和国电子签名法》的推广，我国的电子认证服务业和 PKI 系统的建设应用也进入了新的发展阶段。同时，随着互联网的进一步发展，更多类型的终端接入网络。对于某些类型的终端，如手机、传感器等，由于其计算或通信资源的限制，难以独立完成证书认证路径构造或证书验证，需要 PKI 系统提供代理服务来协助完成上述两种任务。

对于 PKI 依赖方来说，证书认证路径构造和证书验证是必要的过程，但是该过程中所需要的证书查找、撤销信息查找、证书/CRL 验证计算等，需要较大的带宽和计算资源消耗，在计算或通信资源受限的环境下会有不同程度的困难。代理技术是解决上述困难的重要方法，将证书认证路径构造或证书验证委托给代理服务器，能够大大减轻 PKI 客户端的计算负担和通信消耗。

代理认证路径构造和代理验证是两种安全等级不一样的代理服务。对于代理认证路径构造，代理服务器返回验证该证书所需要的完整路径（包括证书链、CRL、OCSP 通信消息等），然后由客户端自己进行验证。这种方式下可以明显减少客户端的通信消耗，且不要求客户端信任服务器；对于代理验证，代理服务器直接返回被验证的证书是否有效。这种方式下客户端的计算负担和通信消耗都明显减少，但客户端应信任代理服务器。为了满足不同交易的安全等级需求，一般要求 PKI 系统同时提供这两种不同的服务。

本标准将定义代理认证路径构造和代理验证两种服务的概念和协议要求，并根据协议要求给出一种标准化的客户端和服务器交互的代理服务协议。

信息安全技术　数字证书代理认证路径构造和代理验证规范

1　范围

本标准规定了数字证书代理认证路径构造和代理验证两种服务的概念和协议要求，以及满足协议要求的代理服务协议。

本标准适用于PKI系统运营机构的代理认证路径构造和代理验证服务的实现和应用。

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 16263.1—2006　信息技术　ASN.1编码规则　第1部分：基本编码规则(BER)、正则编码规则(CER)和非典型编码规则(DER)规范

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

RFC3852　密码消息语法(Cryptographic Message Syntax，CMS)

3　术语和定义

GB/T 16264.8—2005界定的以及以下术语和定义适用于本文件。

3.1

数字证书代理验证　delegated validation for digital certificate

由代理服务器为PKI依赖方实现数字证书验证的过程。

3.2

代理验证　delegated validation

在本标准范围内，与“数字证书代理验证”同义。

3.3

数字证书代理认证路径构造　delegated certification path construction for digital certificate

由代理服务器为PKI依赖方实现数字证书认证路径构造的过程。

3.4

代理认证路径构造　delegated certification path construction

在本标准范围内，与“数字证书代理认证路径构造”同义。

3.5

代理验证策略　delegated validation policy

表达代理验证应如何执行的一系列规则。

3.6

代理认证路径构造策略　delegated certification path construction policy

表达代理认证路径构造应如何执行的一系列规则。