ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30272—2013

信息安全技术　公钥基础设施 标准一致性测试评价指南

Information security technology—Public Key Infrastructure—Testing and evaluation guide on standard conformance

2013-12-31 发布　　2014-07-15 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:公安部计算机信息系统安全产品质量监督检验中心。

本标准主要起草人:邱梓华、顾健、张笑笑、顾玮、邹春明、宋好好、张艳、张岚。

引　言

本标准是用以指导测试评价者，如何测试与评价公钥基础设施是否达到国家标准要求。

本标准依据国家已颁布、实施的6个公钥基础设施标准，即：

——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 19714—2005　信息技术　安全技术　公钥基础设施　证书管理协议

——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

——GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

——GB/T 20519—2006　信息安全技术　公钥基础设施　特定权限管理中心技术规范

——GB/T 20520—2006　信息安全技术　公钥基础设施　时间戳规范

本标准以此6个标准为基础，对相应评价测试方法做了详细描述。对以后新发布的公钥基础设施标准规范，将在修改版本中给出。

信息安全技术　公钥基础设施
标准一致性测试评价指南

1　范围

本标准规定了公钥基础设施相关组件的测试评价指南，涉及CA、RA、终端实体、证书资料库、时间戳子系统、特定权限管理子系统、在线证书状态查询子系统。

本标准适用于按照GB/T 19713—2005、GB/T 19714—2005、GB/T 19771—2005、GB/T 20518—2006、GB/T 20519—2006和GB/T 20520—2006进行研制开发的产品类公钥基础设施相关组件的测试和评价。

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 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 19714—2005　信息技术　安全技术　公钥基础设施　证书管理协议

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

GB/T 20518—2006　信息安全技术　公钥基础设施　数字证书格式

GB/T 20519—2006　信息安全技术　公钥基础设施　特定权限管理中心技术规范

GB/T 20520—2006　信息安全技术　公钥基础设施　时间戳规范

3　术语和定义

GB/T 19713—2005、GB/T 19714—2005、GB/T 19771—2005、GB/T 20518—2006、GB/T 20519—2006和GB/T 20520—2006界定的术语和定义适用于本文件。

4　公钥基础设施测试评价指南

4.1　在线证书状态协议测试评价指南

4.1.1　总则

4.1.1.1　请求

评价内容：

见GB/T 19713—2005中5.2的内容。

对开发者的要求：

a)　开发者应提供文档，对所使用的在线证书状态协议进行说明；

b)　开发者应提供工具模拟不满足条件的请求。

测试评价指南：