ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 30272—2021
代替 GB/T 30272—2013

信息安全技术 公钥基础设施 标准符合性测评

Information security technology—Public key infrastructure—Testing and assessment of compliance with standards

2021-10-11 发布　　2022-05-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　缩略语 …… 1
5　在线证书状态协议测评 …… 2
5.1　总则 …… 2
5.2　安全考虑 …… 4
6　证书管理协议测评 …… 4
6.1　必需的 PKI 管理功能 …… 4
6.2　传输 …… 7
6.3　必选的 PKI 管理消息结构 …… 7
7　组件最小互操作规范测评 …… 8
7.1　组件规范 …… 8
7.2　数据格式 …… 11
8　数字证书格式测评 …… 14
8.1　基本证书域的数据结构 …… 14
8.2　TBSCertificate 及其数据结构 …… 14
8.3　证书扩展项 …… 16
9　时间戳规范测评 …… 21
9.1　时间戳的产生和颁发 …… 21
9.2　时间戳的管理 …… 23
9.3　时间戳的格式 …… 24
9.4　时间戳系统的安全 …… 27
10　电子签名格式测评 …… 29
10.1　基本数据格式 …… 29
10.2　验证数据格式 …… 29
10.3　签名策略要求 …… 30
11　基于数字证书的可靠电子签名生成及验证技术测评 …… 30
11.1　电子签名相关数据的要求 …… 30
11.2　签名生成模块的要求 …… 31
11.3　电子签名生成过程与应用程序要求 …… 31

11.4 电子签名验证过程与应用程序要求 …… 32
12 综合评价 …… 33
附录 A（资料性） 测试项目总表 …… 35
附录 B（资料性） 公钥基础设施测试环境示例 …… 38
参考文献 …… 39

前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

本文件代替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》，与GB/T 30272—2013相比，除编辑性改动外，主要技术变化如下：

——删除了“特定权限管理中心技术规范测评”（见2013年版的4.5）；

——更改了“数字证书格式测评”中的相关内容（见第8章，2013年版的4.4）；

——增加了“电子签名格式测评”（见第10章）；

——增加了“基于数字证书的可靠电子签名生成及验证技术测评”（见第11章）。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC 260）提出并归口。

本文件起草单位：上海辰锐信息科技公司、公安部第三研究所、中国科学院数据与通信保护研究教育中心、北京数字认证股份有限公司、格尔软件股份有限公司、中国电子科技集团公司第十五研究所（信息产业信息安全测评中心）。

本文件主要起草人：邱梓华、陈妍、李谦、刘丽敏、吕娜、郑强、傅大鹏、王路晗、邵旭东、陈家明、顾流、赵欣怡、原泉、刘中、许俊、刘健。

本文件及其所代替文件的历次版本发布情况为：

——2013年首次发布为GB/T 30272—2013；

——本次为第一次修订。

引　言

本文件用于指导测试评价者测试与评价公钥基础设施是否达到国家标准要求。

本文件依据国家已颁布、实施的7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—2018　信息安全技术　公钥基础设施　数字证书格式

——GB/T 20520—2006　信息安全技术　公钥基础设施　时间戳规范

——GB/T 25064—2010　信息安全技术　公钥基础设施　电子签名格式规范

——GB/T 35285—2017　信息安全技术　公钥基础设施　基于数字证书的可靠电子签名生成及验证技术要求

这7个标准对相应评价测试方法做了详细描述。

信息安全技术
公钥基础设施　标准符合性测评

1　范围

本文件描述了公钥基础设施相关组件的测试评价方法，包括CA、RA、时间戳子系统、在线证书状态查询子系统、电子签名及验证子系统、客户端等组件。

本文件适用于按照国家标准GB/T 19713—2005、GB/T 19714—2005、GB/T 19771—2005、GB/T 20518—2018、GB/T 20520—2006、GB/T 25064—2010、GB/T 35285—2017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

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；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—2018　信息安全技术　公钥基础设施　数字证书格式

GB/T 20520—2006　信息安全技术　公钥基础设施　时间戳规范

GB/T 25064—2010　信息安全技术　公钥基础设施　电子签名格式规范

GB/T 25069—2010　信息安全技术　术语

GB/T 35275—2017　信息安全技术　SM2密码算法加密签名消息语法规范

GB/T 35285—2017　信息安全技术　公钥基础设施 基于数字证书的可靠电子签名生成及验证技术要求

3　术语和定义

GB/T 19713—2005、GB/T 19714—2005、GB/T 19771—2005、GB/T 20518—2018、GB/T 20520—2006、GB/T 25064—2010、GB/T 35285—2017、GB/T 25069—2010界定的术语和定义适用于本文件。

4　缩略语

下列缩略语适用于本文件。

BES　基本电子签名(Basis Electronic Signature)

CA　认证机构(Certification Authority)

CPS　认证惯例陈述(Certification Practice Statement)

CRL　证书撤销列表(Certificate Revocation List)