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：

a) 由 OCSP 请求者发送多个不同状态证书的状态请求，检测 OCSP 响应器是否提供了正确的证书状态响应；
b) 检测 OCSP 请求是否包含以下数据：协议颁布、服务请求、目标证书标识符、其他扩展数据（如 OCSP 请求者的签名、随机数等）；
c) 使用工具发送不正确报文格式的请求，检测 OCSP 响应器是否发出错误信息；
d) 使用工具发送响应器没有配置所要求服务的请求，检测 OCSP 响应器是否发出错误信息；
e) 使用工具发送不完整信息的请求，检测 OCSP 响应器是否发出错误信息。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.1.2 响应

评价内容：

见 GB/T 19713—2005 中 5.3 的内容。

对开发者的要求：

开发者应提供文档，对响应签名的密钥、响应消息格式、响应消息内容等进行说明。

测试评价指南：

a) 模拟各种身份的 OCSP 请求者，发送多个不同状态证书的状态请求，OCSP 响应请求，检测此过程中是否对所有明确的响应报文都进行数字签名。
b) 检测响应签名的密钥是否为下列三种情况之一：
   1) 签发待查询证书的 CA；
   2) 可信赖的响应器，即请求者信任该响应器的公钥；
   3) CA 指定的响应器。
c) 由 OCSP 请求者发送多个不同状态证书的状态请求，检测 OCSP 响应器的响应消息中是否包含以下内容：
   1) 响应语法的版本；
   2) 响应器的名称；
   3) 对请求中每个证书的响应；
   4) 可选择的扩展；
   5) 签名算法的 OID；
   6) 响应的哈希签名。
d) 检测对请求中每个证书的响应，是否包含以下内容：
   1) 目标证书标识符；
   2) 证书状态值；
   3) 响应有效期限；
   4) 可选的扩展。
e) 检测 OCSP 响应消息中，证书状态值是否为以下三种响应标识符：
   1) Good，表示对状态查询的肯定响应；
   2) Revoked（已撤销），表示证书已被撤销；
   3) Unknown（未知）：表示不能鉴别待验证状态的证书。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.1.3 异常情况

评价内容：

见 GB/T 19713—2005 中 5.4 的内容。

对开发者的要求：

a) 开发者应提供文档，对 OCSP 响应器返回的错误消息进行说明；

b) 开发者应提供工具模拟各种异常情况。

测试评价指南：

a) 使用工具发送一个没有遵循 OCSP 语法的请求，检测 OCSP 响应器是否发出相应的错误信息；

b) 使响应器处于非协调的工作状态，发送一个正常请求，检测 OCSP 响应器是否发出相应的错误信息；

c) 使响应器处于不能返回所请求证书的状态，发送一个证书请求，检测 OCSP 响应器是否发出相应的错误信息；

d) 使用工具发送一个没有签名的请求，检测 OCSP 响应器是否发出相应的错误信息；

e) 使用工具发送一个未授权的请求，检测 OCSP 响应器是否发出相应的错误信息。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.1.4 thisUpdate、nextUpdate 和 producedAt 的语义

评价内容：

见 GB/T 19713—2005 中 5.5 的内容。

对开发者的要求：

开发者应提供文档，对 thisUpdate、nextUpdate 和 producedAt 的语义进行说明。

测试评价指南：

a) 发送多个证书请求，检测 OCSP 响应消息是否包含以下时间字段：

1) thisUpdate：此次更新时间；

2) nextUpdate(可选字段)：下次更新时间；若没有设置此字段，需指明随时可以获得更新的撤销信息；

3) producedAt：签发时间。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.1.5 OCSP 签名机构的委托

评价内容：

见 GB/T 19713—2005 中 5.7 的内容。

对开发者的要求：

开发者应提供文档，对所使用的在线证书状态协议中 OCSP 签名机构的委托过程进行说明。

测试评价指南：

a) 如果签署证书状态信息的密钥与签署证书的密钥不同，由 CA 向响应器签发一个含有 extendedKeyUsage 唯一值的证书；

b) 发送一个证书状态查询请求，检测响应器能否用上述证书对证书状态信息进行签名。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.1.6 CA 密钥泄露

评价内容：

见 GB/T 19713—2005 中 5.8 的内容。

对开发者的要求：

开发者应提供文档，对 CA 密钥泄露时 OCSP 响应器的设置进行说明。

测试评价指南：

a) 在 OCSP 响应器中，将某一个 CA 的状态设置为私钥泄露；

b) 发送一个上述 CA 签发的证书状态查询请求，检测 OCSP 响应器能否返回证书已撤销的状态信息。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.2 功能要求

4.1.2.1 证书内容

评价内容：

见 GB/T 19713—2005 中 6.1 的内容。

对开发者的要求：

开发者应提供文档，对 CA 的证书相关内容进行说明。

测试评价指南：

a) 检测 CA 是否在 AccessDescription SEQUENCE 中包含 URI accessLocation 值和对象标识符 id-adocsp。

b) 检测 OCSP 响应器的访问位置，是否通过以下两种方式之一给出：

1) 在证书扩展项中提供用于 OCSP 访问的 AuthorityInfoAccess；

2) 在 OCSP 客户端配置。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.2.2 签名响应的接收要求

评价内容：

见 GB/T 19713—2005 中 6.2 的内容。

对开发者的要求：

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。

测试评价指南：

检测在把 OCSP 响应视作有效之前，OCSP 客户端是否确认以下内容：

a) 响应中所鉴别的证书和请求中的证书一致；

b) 响应器的签名是有效的；

c) 响应器的签名者身份和请求的预定接收者一致；

d) 签名者已被授权对响应进行签名；

e) 指明证书状态的时间(thisUpdate)为当前最近的时间；

f) 如果设置了 nextUpdate 字段，此时间晚于客户端当前时间。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.1.3 安全考虑

评价内容：

见 GB/T 19713—2005 中第 8 章的内容。

对开发者的要求：

开发者应提供文档，对所使用的在线证书状态协议进行脆弱性分析。

测试评价指南：

查看开发者提供的脆弱性分析报告，检测 OCSP 系统能否抵御标准中的相关攻击（至少应该包括拒绝服务攻击和重放攻击）。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2 证书管理协议测试评价指南

4.2.1 必需的 PKI 管理功能

4.2.1.1 根 CA 初始化

评价内容：

见 GB/T 19714—2005 中 8.1 的内容。

对开发者的要求：

开发者应提供文档，针对根 CA 初始化的过程进行说明。

测试评价指南：

a) 根据开发者文档，产生一对根 CA 的密钥对，并将密钥对分散保存，检测根密钥的保存方式是否安全；

b) 选择此密钥对进行根 CA 初始化，用产生的私钥为公钥签发证书，产生自己的自签名证书，检测这个证书的结构是否和“newWithNew”证书结构相同；

c) 为 CA 的公钥产生一个指纹，并检测传递指纹的数据结构是否为 OOBCertHash。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.2 根 CA 密钥更新

评价内容：

见 GB/T 19714—2005 中 8.2 的内容。

对开发者的要求：

开发者应提供文档，针对根 CA 密钥更新的过程进行说明。

测试评价指南：

a) 在 CA 的生命周期到期前，模拟一次根 CA 密钥更新的过程；

b) 产生新的根 CA 的密钥对；

c) 产生一个用新私钥为旧公钥签名的证书（“old with new”证书）；

d) 产生一个用旧私钥为新公钥签名的证书（“new with old”证书）；

e) 产生一个用新私钥为新公钥签名的证书（“new with new”证书）；

f) 发布这些新证书；

g) 导出 CA 的新公钥；

h) 使用 CA 的新密钥为一个终端实体签发一个新证书；

i) 利用 CA 旧公钥的终端实体，验证上述新证书，检测验证者是否进行以下操作：在数据库中查找 caCertificate 属性，获得 NewWithOld 证书，并利用 CA 旧密钥验证该 NewWithOld 证书是否正确，如果正确，利用 CA 新密钥验证新证书；

j) 利用 CA 新公钥的终端实体，验证 CA 旧密钥签发的旧证书，检测验证者是否进行以下操作：在数据库中查找 caCertificate 属性，获得 OldWithNew 证书，并利用 CA 新密钥验证该 OldWithNew 证书是否正确，如果正确，利用 CA 旧密钥验证旧证书。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.3 下级 CA 初始化

评价内容：

见 GB/T 19714—2005 中 8.3 的内容。

对开发者的要求：

开发者应提供文档，针对下级 CA 初始化的过程进行说明。

测试评价指南：

a) 在下级 CA 初始化之前，检测下级 CA 能否获得以下 PKI 信息：

1) 当前根 CA 的公钥，并使用哈希值对根 CA 公钥进行带外验证；

2) 撤销列表以及撤销列表的认证路径；

3) 所支持的每一种相关应用的算法和算法变量。

b) 模拟一次下级 CA 初始化的过程：产生下级 CA 密钥，利用根证书产生下级 CA 的签名证书。

c) 产生初始的撤销列表。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.4 CRL 产生

评价内容：

见 GB/T 19714—2005 中 8.4 的内容。

对开发者的要求：

开发者应提供文档，针对 CRL 产生的过程进行说明。

测试评价指南：

a) 在发布证书之前，在新建立 CA 中产生空的 CRL 列表；

b) 检测能否操作成功。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.5 PKI 信息请求

评价内容：

见 GB/T 19714—2005 中 8.5 的内容。

对开发者的要求：

开发者应提供文档，针对 PKI 信息请求进行说明。

测试评价指南：

a) 评价者模拟各种 PKI 信息请求，检测 CA 是否能够向请求者提供至少请求者要求的所有请求信息，如果某些信息不能提供，CA 是否给请求者返回错误信息；

b) 检测文档是否和标准的规定一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.6 交叉认证

评价内容：

见 GB/T 19714—2005 中 8.6 的内容。

对开发者的要求：

开发者应提供文档，针对交叉认证过程进行说明。

测试评价指南：

评价者模拟一次交叉认证过程：

a) 新建三个 CA 系统，分别命名为 A、B、C；

b) 分别使用三个 CA 系统，签发三个证书，分别命名为：a、b、c；

c) 以 CA 系统 A 为请求者，CA 系统 B 为响应者，进行交叉认证操作，检测操作过程和消息结构是否符合标准要求；

d) 在拥有证书 b 的终端实体上，使用交叉认证证书验证证书 a，应能验证成功；

e) 在拥有证书 b 的终端实体上，验证证书 c，验证应不成功。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果系统提供交叉认证功能，以上结果全部正确，则本项满足；如果系统不提供交叉认证功能，在此项不作为最终结果的判断依据。

4.2.1.7 终端实体初始化

4.2.1.7.1 获得 PKI 信息

评价内容：

见 GB/T 19714—2005 中 8.7.1 的内容。

对开发者的要求：

开发者应提供文档，针对终端实体初始化过程中的“获得 PKI 信息”这一步骤进行说明。

测试评价指南：

在终端实体初始化之前，检测能否获得以下 PKI 信息：

a) 当前根 CA 的公钥；

b) 撤销列表以及撤销列表的认证路径；

c) 所支持的每一种相关应用的算法和算法变量。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.7.2 根 CA 密钥的带外验证

评价内容：

见 GB/T 19714—2005 中 8.7.2 的内容。

对开发者的要求：

开发者应提供文档，针对终端实体初始化过程中的“根 CA 密钥的带外验证”这一步骤进行说明。

测试评价指南：

检测系统是否能够通过一些安全的“带外”方法给终端实体提供 CA 的证书指纹。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.8 证书请求

评价内容：

见 GB/T 19714—2005 中 8.8 的内容。

对开发者的要求：

开发者应提供文档，针对证书模板和证书请求进行说明。

测试评价指南：

检测经过初始化的终端实体是否能够请求一个额外的证书：

a) 对每一种证书模板，选择一个经过初始化的终端实体，提出证书请求；

b) 检测这个请求是否使用认证请求(cr)消息；

c) 检测能否返回新的证书；

d) 选择一个已经拥有一对签名密钥(带有相应的验证证书)的终端实体，提出证书请求；

e) 检测请求(cr)消息是否使用此实体的数字签名来保护；

f) 检测能否返回新的证书；

g) 检查文档是否和标准的规定一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.1.9 密钥更新

评价内容：

见 GB/T 19714—2005 中 8.9 的内容。

对开发者的要求：

开发者应提供文档，针对密钥更新进行说明。

测试评价指南：

a) 在终端实体的证书将要过期前，评价者模拟密钥更新的过程；

b) 检查文档是否和标准的规定一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.2 传输

评价内容：

见 GB/T 19714—2005 中第 9 章的内容。

对开发者的要求：

开发者应提供文档，说明在 EE、RAs、CAs 之间传输 PKI 消息的传输协议和消息格式。

测试评价指南：

a) 如果 PKI 消息通过文件传输，检测 PKI 消息的格式是否符合标准要求；

b) 如果 PKI 消息通过 TCP 管理协议传输，检测 PKI 消息的格式是否符合标准要求；

c) 如果 PKI 消息通过 E-mail 方式传输，检测 PKI 消息的格式是否符合标准要求；

d) 如果 PKI 消息通过 HTTP 方式传输，检测 PKI 消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果系统支持的每种传输方式的消息格式和传输协议均符合标准要求，则本项满足。

4.2.3 必选的 PKI 管理消息结构

4.2.3.1 初始的注册/认证(基本认证方案)

评价内容：

见 GB/T 19714—2005 中 B.4 的内容。

对开发者的要求：

开发者应提供文档，说明初始的注册/认证的消息格式。

测试评价指南：

通过未初始化的终端实体向 CA 请求第一个证书，根据开发者所提供的文档，检测终端实体和 PKI 之间的通信消息是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.3.2 证书请求

评价内容：

见 GB/T 19714—2005 中 B.5 的内容。

对开发者的要求：

开发者应提供文档，说明证书请求的消息格式。

测试评价指南：

通过已经初始化的终端实体向 CA 请求证书，根据开发者所提供的文档，检测终端实体和 PKI 之间的通信消息是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.2.3.3 密钥更新请求

评价内容：

见 GB/T 19714—2005 中 B.6 的内容。

对开发者的要求：

开发者应提供文档，说明密钥更新请求的消息格式。

测试评价指南：

在密钥即将过期前，通过已经初始化的终端实体向 CA 请求证书(用于更新密钥对和/或已经拥有的相应证书)，根据开发者所提供的文档，检测终端实体和 PKI 之间的通信消息是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3 PKI 组件最小互操作规范测试评价指南

4.3.1 PKI 组件规范

4.3.1.1 证书认证机构(CA)

4.3.1.1.1 颁发数字签名证书

评价内容：

见 GB/T 19771—2005 中 5.2.2 a)的内容。

对开发者的要求：

开发者应提供文档，针对数字签名证书的颁发进行说明。

测试评价指南：

a) 对每一种证书模板，通过授权 RA 产生多个签名数字证书请求，并发送给 CA，检测 CA 能否生

成新证书并将其放在资料库中；

b) 通过非授权 RA 产生一个签名数字证书请求，并发送给 CA，检测 CA 能否拒绝该证书申请，能否向 RA 报告失败并说明原因；

c) 通过授权 RA 产生一个包含不匹配信息的签名数字证书请求，并发送给 CA，检测 CA 能否拒绝该证书申请，能否向 RA 报告失败并说明原因；

d) 对每一种证书模板，产生多个自我注册的证书请求，并发送给 CA，检测 CA 是否验证请求者的身份并验证申请者的相应私钥，如果验证成功，检测 CA 能否生成新证书并将其放在资料库中；如果验证失败，检测 CA 能否拒绝该证书申请，能否向申请者报告失败并说明原因；

e) 对每一种证书模板，产生多个更新的证书请求，并发送给 CA，检测 CA 是否验证请求者的身份，如果验证成功，检测 CA 能否生成新证书并将其放在资料库中；如果签名无效或者 CA 策略不允许更新，检测 CA 能否拒绝该证书更新请求，并向申请者报告失败并说明原因；

f) 以非法的请求者产生一个更新的证书请求，检测 CA 能否拒绝该证书更新请求，能否向申请者报告失败并说明原因。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.1.1.2 颁发加密证书

评价内容：

见 GB/T 19771—2005 中 5.2.2 b)的内容。

对开发者的要求：

开发者应提供文档，针对加密证书的颁发进行说明。

测试评价指南：

a) 由第三方集中产生加密密钥对，并通过带外方式提供给 CA；

b) 由证书持有者生成多个加密证书请求，说明自己想要的加密算法，并对该请求进行数字签名，将该请求发送给 CA；

c) 检测 CA 能否验证请求者身份，并颁发加密证书和加密密钥给请求者。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.1.1.3 交叉认证

评价内容：

见 GB/T 19771—2005 中 5.2.2 c)的内容。

对开发者的要求：

开发者应提供文档，针对 CA 间的交叉认证进行说明。

测试评价指南：

a) 在两个交叉认证的 CA 之间交换 CA 的公钥，分别为对方的公钥生成证书，并将其存放到资料库中；

b) 检测双方之间的证书能否交叉认证。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果系统提供交叉认证功能，以上结果全部正确，则本项满足；如果系统不提供交叉认证功能，在此项不作为最终结果的判断依据。

4.3.1.1.4 撤销证书

评价内容：

见 GB/T 19771—2005 中 5.2.2d)的内容。

对开发者的要求：

开发者应提供文档，针对证书的撤销进行说明。

测试评价指南：

a) 以多个证书持有者身份请求撤销证书，并将请求发送给 CA，检测 CA 是否验证请求者身份，验证成功后能否将证书放入 CRL 中；

b) 检测新的 CRL 产生时，老 CRL 中的全部信息是否放到新 CRL 中；

c) 通过 RA 向 CA 发送多个证书撤销请求，检测 CA 是否验证请求者身份，验证成功后能否将证书放入 CRL 中。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.1.1.5 请求 CA 证书

评价内容：

见 GB/T 19771—2005 中 5.2.2f)的内容。

对开发者的要求：

开发者应提供文档，针对向更高层次 CA 申请证书进行说明。

测试评价指南：

通过 CA 向层次更高的 CA 申请证书，检测能否申请成功。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.1.2 注册机构(RA)

评价内容：

见 GB/T 19771—2005 中 5.3 的内容。

对开发者的要求：

开发者应提供文档，针对 RA 的操作规范进行说明。

测试评价指南：

a) 针对每一种证书模板，向 RA 提交多个 CertReq 格式的证书请求；

b) 检测 RA 是否审查请求者的身份；

c) 检测 RA 是否确认请求者是否拥有相应的完整的密钥对；

d) 验证通过后，检测 RA 能否抽取公钥信息并用 RA 的名字和签名建立一个新的 CertReq 消息；

e) 检测 RA 能否将新的 CertReq 消息发送给 CA；

f) 如果证书请求被接受，检测 RA 能否接收 CA 颁发的新证书，并将新证书发送给请求者；

g) 如果证书请求被拒绝，检测 RA 能否审查从 CA 发来的错误代码；

h) 向 RA 提交多个证书撤销请求，检测 RA 是否验证请求者身份，并产生新的 RevReq 消息；

i) 检测 RA 能否将新的 RevReq 消息发送给 CA；

j) 如果证书撤销请求被接受，检测 RA 能否接收 CA 回应的 RevReq 消息，能否将此信息提交给请求者；

k) 如果证书撤销请求被拒绝，检测 RA 能否审查错误代码，并再次产生撤销请求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.1.3 证书持有者规范

评价内容：

见 GB/T 19771—2005 中 5.4 的内容。

对开发者的要求：

开发者应提供文档，针对证书持有者规范进行说明。

测试评价指南：

a) 以多个用户身份申请签名证书，检测能否成功申请并且获取证书；

b) 以多个用户身份申请加密证书，检测能否成功申请并且获取证书；

c) 以多个证书持有者身份，申请撤销签名证书，检测能否成功撤销证书；

d) 以多个证书持有者身份，申请更新签名证书，检测能否成功更新证书。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.1.4 客户规范

评价内容：

见 GB/T 19771—2005 中 5.5 的内容。

对开发者的要求：

开发者应提供文档，针对客户规范进行说明。

测试评价指南：

a) 验证客户能否验证签名；

b) 验证客户能否从查询服务器检索证书和 CRLs；

c) 验证客户能否验证证书认证路径。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2 数据格式

4.3.2.1 证书撤销列表

评价内容：

见 GB/T 19771—2005 中 6.3 的内容。

对开发者的要求：

开发者应提供文档，针对证书撤销列表的格式进行说明。

测试评价指南：

a) 由 CA 颁发证书撤销列表；

b) 下载证书撤销列表，检测证书撤销列表的格式是否符合标准要求；

c) 多次进行上述操作。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.2 事务消息格式

4.3.2.2.1 全体 PKI 消息组件

评价内容：

见 GB/T 19771—2005 中 6.5.2 的内容。

对开发者的要求：

开发者应提供文档，针对 PKI 消息的格式进行说明。

测试评价指南：

根据开发者提供的文档，检测 PKI 消息（包括：header、body、protection、extraCerts 字段）的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.2.2 通用数据结构

评价内容：

见 GB/T 19771—2005 中 6.5.3 的内容。

对开发者的要求：

开发者应提供文档，针对证书模板、签名私钥的拥有证明、证书请求消息、协议加密密钥控制、PKI 消息状态码、失败信息、确认协议、证书识别、Centrally Generated Keys 和带外信息的格式进行说明。

测试评价指南：

a) 根据开发者提供的文档，检测证书模板的消息格式是否符合标准要求；

b) 根据开发者提供的文档，检测签名私钥的拥有证明消息格式是否符合标准要求；

c) 根据开发者提供的文档，检测证书请求的消息格式是否符合标准要求；

d) 根据开发者提供的文档，检测协议加密密钥控制的消息格式是否符合标准要求；

e) 根据开发者提供的文档，检测 PKI 消息状态码的消息格式是否符合标准要求；

f) 根据开发者提供的文档，检测失败信息的消息格式是否符合标准要求；

g) 根据开发者提供的文档，检测确认协议的消息格式是否符合标准要求；

h) 根据开发者提供的文档，检测证书识别的消息格式是否符合标准要求；

i) 根据开发者提供的文档，检测 Centrally Generated Keys 的消息格式是否符合标准要求；

j) 根据开发者提供的文档，检测带外信息的消息格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.2.3 特殊操作的数据结构

评价内容：

见 GB/T 19771—2005 中 6.5.4 的内容。

对开发者的要求：

开发者应提供文档，针对注册/证书请求、注册/证书响应、撤销请求的内容、撤销响应内容、PKCS＃10 证书请求的消息格式进行说明。

测试评价指南：

a) 根据开发者提供的文档，检测注册/证书请求的消息格式是否符合标准要求；

b) 根据开发者提供的文档，检测注册/证书响应的拥有证明消息格式是否符合标准要求；

c) 根据开发者提供的文档，检测撤销请求的内容的消息格式是否符合标准要求；

d) 根据开发者提供的文档，检测撤销响应内容的消息格式是否符合标准要求；

e) 根据开发者提供的文档，检测 PKCS＃10 证书请求的消息格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3 PKI 事务

4.3.2.3.1 RA 发起的注册请求

评价内容：

见 GB/T 19771—2005 中 6.6.2 的内容。

对开发者的要求：

如果产品支持远端 RA，则开发者应提供文档，针对 RA 发起的注册请求进行说明。

测试评价指南：

a) 根据开发者提供的文档，对每一种证书模板，在远端 RA 上向 CA 请求多个终端实体的证书；

b) 检测从 RA 到 CA 的证书请求消息的格式是否符合标准要求；

c) 检测从 CA 到 RA 的证书回应消息的格式是否符合标准要求；

d) 检测确认消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.2 新实体的自我注册请求

评价内容：

见 GB/T 19771—2005 中 6.6.3 的内容。

对开发者的要求：

如果 CA 接受自我注册请求，则开发者应提供文档，针对新实体的自我注册请求进行说明。

测试评价指南：

a) 根据开发者提供的文档，对每一种证书模板，以多个新实体身份直接向 CA 申请新的证书；

b) 检测从证书持有者到 CA 的自我注册请求消息的格式是否符合标准要求；

c) 检测从 CA 到证书请求者的自我注册请求回应消息的格式是否符合标准要求；

d) 检测确认消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.3 已知实体的自我注册请求

评价内容：

见 GB/T 19771—2005 中 6.6.4 的内容。

对开发者的要求：

如果 CA 接受自我注册请求，则开发者应提供文档，针对已知实体的自我注册请求进行说明。

测试评价指南：

a) 根据开发者提供的文档，对每一种证书模板，以多个已知实体身份直接向 CA 申请新的证书；

b) 检测从证书持有者到 CA 的自我注册请求消息的格式是否符合标准要求；

c) 检测从 CA 到证书请求者的自我注册请求回应消息的格式是否符合标准要求；

d) 检测确认消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.4 证书更新

评价内容：

见 GB/T 19771—2005 中 6.6.5 的内容。

对开发者的要求：

如果 CA 的 CPS 支持证书更新，则开发者应提供文档，针对证书的更新进行说明。

测试评价指南：

a) 根据开发者提供的文档，对每一种证书模板，以多个拥有当前有效证书的实体身份直接向 CA 申请新的证书；

b) 检测从证书持有者到 CA 的证书更新申请消息的格式是否符合标准要求；

c) 检测从 CA 到证书持有者的自证书更新响应消息的格式是否符合标准要求；

d) 检测确认消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.5 PKCS＃10 自我注册请求

评价内容：

见 GB/T 19771—2005 中 6.6.6 的内容。

对开发者的要求：

如果 CA 接受自我注册请求，则开发者应提供文档，针对 PKCS＃10 自我注册请求进行说明。

测试评价指南：

a) 根据开发者提供的文档，对每一种证书模板，以多个新实体身份直接向 CA 申请新的 PKCS＃10 证书；

b) 检测从证书持有者到 CA 的自我注册请求消息的格式是否符合标准要求；

c) 检测从 CA 到证书请求者的 PKCS 证书请求响应消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.6 撤销请求

评价内容：

见 GB/T 19771—2005 中 6.6.7 的内容。

对开发者的要求：

开发者应提供文档，针对撤销请求进行说明。

测试评价指南：

a) 根据开发者提供的文档，以多个拥有当前有效证书的实体身份直接申请撤销自己的证书；

b) 检测从证书持有者到 RA 的撤销请求消息的格式是否符合标准要求；

c) 检测从 RA 到 CA 的撤销请求消息的格式是否符合标准要求；

d) 检测从 CA 到 RA 的撤销响应消息的格式是否符合标准要求；

e) 检测从 RA 到证书持有者的撤销响应消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.7 集中产生密钥对和密钥管理证书申请

评价内容：

见 GB/T 19771—2005 中 6.6.8 的内容。

对开发者的要求：

开发者应提供文档，针对集中产生密钥对和密钥管理证书申请进行说明。

测试评价指南：

a） 根据开发者提供的文档，以多个拥有当前有效证书的实体身份向 CA 申请产生加密密钥并签发证书；

b） 检测集中产生密钥对申请消息的格式是否符合标准要求；

c） 检测集中产生密钥对回应消息的格式是否符合标准要求；

d） 检测确认消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.3.2.3.8 组合证书申请

评价内容：

见 GB/T 19771—2005 中 6.6.9 的内容。

对开发者的要求：

如果 CA 支持组合证书，则开发者应提供文档，针对组合证书申请进行说明。

测试评价指南：

a） 根据开发者提供的文档，以多个新实体身份向 CA 申请组合证书：一个签名密钥证书和加密证书；

b） 检测组合证书申请消息的格式是否符合标准要求；

c） 检测组合证书回应消息的格式是否符合标准要求；

d） 检测确认消息的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4 数字证书格式测试评价指南

4.4.1 基本证书域的数据结构

评价内容：

见 GB/T 20518—2006 中 5.2.1 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 对每一种证书模板，使用公钥基础设施颁发多个数字证书；

b） 检测所颁发数字证书的基本数据结构是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.2 TBSCertificate 及其数据结构

4.4.2.1 版本 version

评价内容：

见 GB/T 20518—2006 中 5.2.2.1 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 检测所颁发数字证书中是否包含版本项；

b） 检测证书中版本项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.2.2 序列号 serial number

评价内容：

见 GB/T 20518—2006 中 5.2.2.2 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 检测所颁发数字证书中是否包含序列号项；

b） 检测证书中序列号项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.2.3 签名算法 signature

评价内容：

见 GB/T 20518—2006 中 5.2.2.3 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 检测所颁发数字证书中是否包含签名算法项；

b） 检测证书中签名算法项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.2.4 颁发者 issuer

评价内容：

见 GB/T 20518—2006 中 5.2.2.4 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 检测所颁发数字证书中是否包含颁发者项；

b） 检测证书中颁发者项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.2.5 有效期 validity

评价内容：

见 GB/T 20518—2006 中 5.2.2.5 的内容。

对开发者的要求：

开发者应提供文档,针对所颁发的数字证书格式进行说明。

测试评价指南:

a) 检测所颁发数字证书中是否包含有效期项;

b) 检测证书中有效期项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.4.2.6 主体 subject

评价内容:

见 GB/T 20518—2006 中 5.2.2.6 的内容。

对开发者的要求:

开发者应提供文档,针对所颁发的数字证书格式进行说明。

测试评价指南:

a) 检测所颁发数字证书中是否包含主体项;

b) 检测证书中主体项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.4.2.7 主体公钥信息 Subject Public Key Info

评价内容:

见 GB/T 20518—2006 中 5.2.2.7 的内容。

对开发者的要求:

开发者应提供文档,针对所颁发的数字证书格式进行说明。

测试评价指南:

a) 检测所颁发数字证书中是否包含主体公钥信息项;

b) 检测证书中主体公钥信息项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.4.2.8 颁发者唯一标识符 IssuerUniqueID

评价内容:

见 GB/T 20518—2006 中 5.2.2.8 的内容。

对开发者的要求:

开发者应提供文档,针对所颁发的数字证书格式进行说明。

测试评价指南:

a) 检测所颁发数字证书中是否未包含颁发者唯一标识符项;

b) 记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.4.2.9 主体唯一标识符 SubjectUniqueID

评价内容:

见 GB/T 20518—2006 中 5.2.2.9 的内容。

对开发者的要求:

开发者应提供文档,针对所颁发的数字证书格式进行说明。
测试评价指南:
检测所颁发数字证书中是否未包含主体唯一标识符项。
记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。
如果以上结果全部正确,则本项满足。

4.4.3 证书扩展项

4.4.3.1 标准扩展

4.4.3.1.1 颁发机构密钥标识符 authorityKeyIdentifier

评价内容:
见 GB/T 20518—2006 中 5.2.3.2.1 的内容。
对开发者的要求:
开发者应提供文档,针对所颁发的数字证书格式进行说明。
测试评价指南:
a) 检测所颁发数字证书中是否包含颁发机构密钥标识符项;
b) 检测证书中颁发机构密钥标识符项的格式、内容是否和标准一致。
记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。
如果以上结果全部正确,则本项满足。

4.4.3.1.2 主体密钥标识符 subjectKeyIdentifier

评价内容:
见 GB/T 20518—2006 中 5.2.3.2.2 的内容。
对开发者的要求:
开发者应提供文档,针对所颁发的数字证书格式进行说明。
测试评价指南:
a) 检测所颁发数字证书中是否包含主体密钥标识符项;
b) 检测证书中主体密钥标识符项的格式、内容是否和标准一致。
记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。
如果以上结果全部正确,则本项满足。

4.4.3.1.3 密钥用法 keyUsage

评价内容:
见 GB/T 20518—2006 中 5.2.3.2.3 的内容。
对开发者的要求:
开发者应提供文档,针对所颁发的数字证书格式进行说明。
测试评价指南:
a) 检测所颁发数字证书中是否包含密钥用法项;
b) 检测证书中密钥用法项的格式、内容是否和标准一致。
记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。
如果以上结果全部正确,则本项满足。

4.4.3.1.4 扩展密钥用途 extKeyUsage

评价内容:

见 GB/T 20518—2006 中 5.2.3.2.4 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持扩展密钥用途扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含扩展密钥用途项；

c） 检测证书中扩展密钥用途项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.5 私有密钥使用期 privateKeyUsagePeriod

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.5 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持私有密钥使用期扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含私有密钥使用期项；

c） 检测证书中私有密钥使用期项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.6 证书策略 certificatePolicies

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.6 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 检测所颁发数字证书中是否包含证书策略项；

b） 检测证书中证书策略项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.7 策略映射 policyMappings

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.7 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持策略映射扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含策略映射项；

c） 检测证书中策略映射项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.8 主体替换名称 subjectAltName

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.8 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果证书中的唯一主体身份是一个选择名称格式（如一个电子邮件地址），主体的甄别名为空序列，则本项为检测项目，否则为非检测项；

b) 检测证书中主体替换名称项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.9 颁发者替换名称 issuerAltName

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.9 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持颁发者替换名称扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含颁发者替换名称项；

c) 检测证书中颁发者替换名称项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.10 主体目录属性 subjectDirectoryAttributes

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.10 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持主体目录属性扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含主体目录属性项；

c) 检测证书中主体目录属性项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.11 基本限制 basicConstraints

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.11 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 检测所颁发数字证书中是否包含基本限制项；

b） 检测证书中基本限制项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.12 名称限制 nameConstraints

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.12 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持名称限制扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含名称限制项；

c） 检测证书中名称限制项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.13 策略限制 policyConstraints

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.13 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持策略限制扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含策略限制项；

c） 检测证书中策略限制项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.14 证书撤销列表分发点 CRLDistributionPoints

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.14 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持证书撤销列表分发点扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含证书撤销列表分发点项；

c） 检测证书中证书撤销列表分发点项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.15 限制所有策略 inhibitAnyPolicy

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.15 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持限制所有策略扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含限制所有策略项；

c） 检测证书中限制所有策略项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.16 最新证书撤销列表 freshestCRL

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.16 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持最新证书撤销列表扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含最新证书撤销列表项；

c） 检测证书中最新证书撤销列表项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.17 个人身份标识码 IdentifyCode

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.17 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持个人身份标识码扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含个人身份标识码项；

c） 检测证书中个人身份标识码项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.18 个人社会保险号 InsuranceNumber

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.18 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a） 如果公钥基础设施支持个人社会保险号扩展项，则此项为检测项，否则为非检测项；

b） 检测所颁发数字证书中是否包含个人社会保险号项；

c） 检测证书中个人社会保险号项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.19 企业工商注册号 ICRegistrationNumber

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.19 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持企业工商注册号扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含企业工商注册号项；

c) 检测证书中企业工商注册号项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.20 企业组织机构代码 OrganizationCode

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.20 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持企业组织机构代码扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含企业组织机构代码项；

c) 检测证书中企业组织机构代码项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.1.21 企业税号 TaxationNumber

评价内容：

见 GB/T 20518—2006 中 5.2.3.2.21 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持企业税号扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含企业税号项；

c) 检测证书中企业税号项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.2 专用因特网扩展 PrivateInternetExtensions id-pkix

4.4.3.2.1 机构信息访问 authorityInfoAccess

评价内容：

见 GB/T 20518—2006 中 5.2.3.3.1 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持机构信息访问扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含机构信息访问项；

c) 检测证书中机构信息访问项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.4.3.2.2 主体信息访问 SubjectInformationAccess

评价内容：

见 GB/T 20518—2006 中 5.2.3.3.2 的内容。

对开发者的要求：

开发者应提供文档，针对所颁发的数字证书格式进行说明。

测试评价指南：

a) 如果公钥基础设施支持主体信息访问扩展项，则此项为检测项，否则为非检测项；

b) 检测所颁发数字证书中是否包含主体信息访问项；

c) 检测证书中主体信息访问项的格式、内容是否和标准一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5 特定权限管理中心技术规范测试评价指南

4.5.1 系统相关协议

4.5.1.1 代理点 PA 与属性注册机构 ARA 间的通信协议

4.5.1.1.1 功能支持

评价内容：

见 GB/T 20519—2006 中 6.1.2 的内容。

对开发者的要求：

开发者应提供文档，针对协议所支持的操作功能进行说明。

测试评价指南：

a) 如代理点 PA 与属性注册机构 ARA 采用在线方式，则本项为检测项目，否则为非检测项；

b) 通过 PA 申请多个属性证书，检测 ARA 能否对申请的属性证书进行注册；

c) 通过 ARA 对各种类型的注册信息进行分析、鉴别，检测 ARA 能否给予认可或不认可的决定；

d) 检测 ARA 能否对注册信息进行修改；

e) 检测 ARA 能否对已经生效的有效证书进行撤销。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.1.1.2 PA 与 ARA 之间的认证机制

评价内容：

见 GB/T 20519—2006 中 6.1.3 的内容。

对开发者的要求：

开发者应提供文档，针对 PA 与 ARA 之间的认证机制进行说明。

测试评价指南：

a) 如代理点 PA 与属性注册机构 ARA 采用在线方式，则本项为检测项目，否则为非检测项；

b) 根据开发者提供的文档，检测 PA 与 ARA 之间是否采用安全认证机制；

c) 以合法的实体身份请求属性证书，检测 ARA 能否对请求的实体身份进行强鉴别；

d) 检测 PA 与 ARA 之间的强鉴别机制是否符合 GB/T 20519—2006 附录 B 中 B.1 的要求；

e) 以非法的实体身份请求属性证书，检测 ARA 能否对请求的实体身份进行强鉴别。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.1.1.3 PA 数据签名

评价内容：

见 GB/T 20519—2006 中 6.1.4 的内容。

对开发者的要求：

开发者应提供文档，针对 PA 提交数据的签名过程进行说明。

测试评价指南：

a) 如代理点 PA 与属性注册机构 ARA 采用在线方式，则本项为检测项目，否则为非检测项；

b) 检测 PA 是否对提交的数据，进行数字签名；

c) 检测签名数据的内容是否符合 GB/T 20519—2006 附录 B 中 B.2 的要求；

d) 检测接收者是否验证所提交数据的签名。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.1.2 属性注册机构 ARA 与属性授权机构 AA 间的通信协议

评价内容：

见 GB/T 20519—2006 中 6.2 的内容。

对开发者的要求：

开发者应提供文档，针对 ARA 与 AA 间的通信协议进行说明。

测试评价指南：

a) 如属性注册机构 ARA 与属性授权机构 AA 采用在线申请方式，则本项为检测项目，否则为非检测项；

b) 检测 AA 和 ARA 之间，是否采用双向强鉴别机制进行网络连接；

c) 检测 AA 和 ARA 之间的双向强鉴别机制是否符合 GB/T 20519—2006 附录 B 中 B.4 的要求；

d) 由 ARA 向 AA 提交一个属性证书的签发请求，检测请求的内容是否包括：标识名称、待签发实体公钥证书、实体属性集、待签发实体对实体属性集的签名和由请求证书实体对上述内容的完整签名；

e) 检测 AA 是否请求实体进行鉴别；

f) 检测 AA 是否验证签发实体的公钥证书；

g) 检测 AA 是否验证实体签名；

h) 如果一切合法，由 AA 签发一个属性证书，并将签发的属性证书发布出去；

i) 检测签发的属性证书是否符合 GB/T 20519—2006 附录 A 的要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.1.3 属性授权机构 AA 与认证机构源 SOA 间的通信协议

评价内容：

见 GB/T 20519—2006 中 6.3 的内容。

对开发者的要求：

开发者应提供文档，针对 AA 与 SOA 间的通信协议进行说明。

测试评价指南：

a) 如果 AA 与 SOA 间采用离线方式，将 AA 的公钥证书、必要批件、填写的属性权限申请表提交给 SOA，检测 SOA 能否授予 AA 相匹配的权限、管理策略，能否签发属性授权证书、策略证书；

b) 如果 AA 与 SOA 间采用在线申请方式，将 AA 的公钥证书、批件号和申请材料在线发送给 SOA，检测 AA 和 SOA 之间是否进行双向强鉴别。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.2 PMI/AA 的安全实施

4.5.2.1 证书撤销安全

评价内容：

见 GB/T 20519—2006 中 8.1 的内容。

对开发者的要求：

开发者应提供文档，针对属性证书失效后的证书撤销措施进行说明。

测试评价指南：

a) 颁发一个长周期的属性证书，并更改时间使其失效；

b) 在 ARA 和 AA 上设置自动监测管理；

c) 失效的属性证书应及时被撤销。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.2.2 算法强度安全

评价内容：

见 GB/T 20519—2006 中 8.2 的内容。

对开发者的要求：

开发者应提供文档，针对属性证书的算法强度进行说明。

测试评价指南：

a) 检查属性证书的加密算法是否得到国家密码管理部门的认可；

b) 颁发一个属性证书，检测在 AC 所有者和属性间的绑定，是否和批准算法一致。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.2.3 身份标识安全

评价内容：

见 GB/T 20519—2006 中 8.3 的内容。

对开发者的要求：

开发者应提供文档，针对属性证书的身份标识进行说明。

测试评价指南：

颁发多个属性证书，检测属性证书中的 holder.entityName 项，是否编码以区分姓名。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.2.4 LDAP 服务访问安全

评价内容：

见 GB/T 20519—2006 中 8.4 的内容。

对开发者的要求：

开发者应提供文档，针对属性证书的 LDAP 访问控制进行说明。

测试评价指南：

a) 在 PMI/AA 系统中，分别以不同授权的用户访问发布属性证书的 LDAP 服务器，检测能否获取授权范围内的属性证书；

b) 尝试获取授权范围以外的属性证书，检测能否获取成功。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.2.5 属性内容安全

评价内容：

见 GB/T 20519—2006 中 8.5 的内容。

对开发者的要求：

开发者应提供文档，针对属性证书的内容安全进行说明。

测试评价指南：

a) 如果属性证书被完整地包含在应用协议中，或者属性证书包含敏感信息，则必须对属性证书加密；

b) 检测属性证书的密文内容和密文格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.5.3 属性证书格式

评价内容：

见 GB/T 20519—2006 中附录 A 的内容。

对开发者的要求：

开发者应提供文档，针对属性证书的格式进行说明。

测试评价指南：

检测属性证书的结构、内容、扩展域和互斥扩展域的格式是否符合标准要求。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6 时间戳规范测试评价指南

4.6.1 时间戳的产生和颁发

4.6.1.1 申请和颁发方式

评价内容：

见 GB/T 20520—2006 中 6.1 的内容。

对开发者的要求：

开发者应提供文档，针对进行说明。

测试评价指南：

a) 根据开发者提供的时间戳申请和颁发方式，向 TSA 申请时间戳；

b) 检测 TSA 是否向申请者返回时间戳。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.1.2 可信时间的产生方法

评价内容：

见 GB/T 20520—2006 中 6.2 的内容。

对开发者的要求：

开发者应提供文档，针对可信时间的产生方法进行说明。

测试评价指南：

检测 TSA 能否按规定方式获得时间。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.1.3 时间的同步

评价内容：

见 GB/T 20520—2006 中 6.3 的内容。

对开发者的要求：

开发者应提供文档，针对时间同步的措施和步骤进行说明。

测试评价指南：

a) 在获得可信时间后，检测 TSA 能否对所有部件的时间进行调整；

b) 检测 TSA 能否在规定时间间隔内定期同步时间；

c) 调整时间同步的间隔时间，检测 TSA 能否在规定时间间隔内定期同步时间；

d) 检测 TSA 各个部件是否采取统一行动同步时间；

e) 检测可信时间源是否为第一个启动的部件；

f) 检测在 TSA 开始工作之前，是否进行了时间同步；

g) 在定期同步时间的过程中，模拟无法获得可信时间的情况，检测 TSA 是否立即停止接受时间戳申请和时间同步，检测是否向管理者发出警报并写入审计日志；

h) 在定期同步时间的过程中，模拟篡改时间信息的情况，检测 TSA 是否立即停止接受时间戳申请和时间同步，检测是否向管理者发出警报并写入审计日志。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.1.4 申请和颁发过程

评价内容：

见 GB/T 20520—2006 中 6.4 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳的申请和颁发过程进行说明。

测试评价指南：

a) 向 TSA 提交时间戳申请请求，检测请求消息的格式是否符合标准；

b) 提交一个不合法的请求信息，检测 TSA 是否产生一个时间戳的失败响应，检测 TSA 是否填写申请被拒绝的原因；

c) 提交一个合法的请求信息，并且使 TSA 无法颁发这个时间戳，检测 TSA 是否产生一个时间戳的失败响应，检测 TSA 是否填写申请被拒绝的原因；

d) 提交一个合法的请求信息，并且 TSA 运行正常，检测 TSA 能否颁发一个格式正确的时间戳并签名；

e) 检测 TSA 签名系统是否通过可信通道把新生成的时间戳发送给时间戳数据库，并由时间戳数据库将其归档保存；

f) 使 TSA 系统将合法的时间戳按规定方式发给用户，检测能否发送成功；在收到合法的时间戳后，检测用户是否验证时间戳的合法性；

g) 使 TSA 系统将不合法或错误的时间戳按规定方式发给用户，检测能否发送成功；在收到不合法或错误的时间戳后，检测用户能否验证出不合法或错误的时间戳；检测用户是否立即向 TSA 管理者报告异常情况；

h) 检测 TSA 对 g)中的情况是否有完备的处理预案，并检测处理预案的可行性。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.2 时间戳的管理

4.6.2.1 时间戳的保存

4.6.2.1.1 在 TSA 方的保存

评价内容：

见 GB/T 20520—2006 中 7.1.1 的内容。

对开发者的要求：

开发者应提供文档，针对 TSA 系统中时间戳的保存进行说明。

测试评价指南：

a) 根据说明，检测 TSA 系统是否保存了所有颁发的时间戳；

b) 检测是否保存了时间戳的以下信息:入库时间、序列号、完整编码。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.6.2.1.2 在用户方的保存

评价内容:

见 GB/T 20520—2006 中 7.1.2 的内容。

对开发者的要求:

开发者应提供文档,针对进行说明。

测试评价指南:

用户在收到时间戳后,检测能否以文件的形式保存时间戳。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.6.2.2 时间戳的备份

评价内容:

见 GB/T 20520—2006 中 7.2 的内容。

对开发者的要求:

开发者应提供文档,针对时间戳的备份进行说明。

测试评价指南:

a) 检测时间戳的备份是否使用异地备份的方式;

b) 检测开发者是否采取严格的措施保护时间戳的备份介质,防止备份介质被盗、被毁和受损;

c) 检测时间戳的备份数据是否以方便检索的方式存放。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.6.2.3 时间戳的检索

评价内容:

见 GB/T 20520—2006 中 7.3 的内容。

对开发者的要求:

开发者应提供文档,针对时间戳的检索进行说明。

测试评价指南:

a) 检测 TSA 是否提供一个时间戳检索的方式;

b) 检测 TSA 是否提供现存以及备份的时间戳以供检索;

c) 检测 TSA 能否通过时间戳入库的时间进行检索;

d) 检测 TSA 能否通过时间戳的序列号进行检索;

e) 检测 TSA 能否通过时间戳的完整编码进行检索;

f) 检测时间戳的检索结果能否发送给用户。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确,则本项满足。

4.6.2.4 时间戳的删除和销毁

4.6.2.4.1 时间戳的删除

评价内容:

见 GB/T 20520—2006 中 7.4.1 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳的删除进行说明。

测试评价指南：

a） 以 TSA 管理员身份登录系统，备份要删除的时间戳，然后删除此时间戳，检测能否删除成功；

b） 以非授权用户身份登录系统，尝试删除时间戳，检测能否删除成功。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.2.4.2 时间戳的销毁

评价内容：

见 GB/T 20520—2006 中 7.4.2 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳的销毁进行说明。

测试评价指南：

a） 在 TSA 证书失效前，尝试销毁所有时间戳，检测能否销毁成功；

b） 在 TSA 证书失效后，并且超过了规定的保存时间，以非授权用户身份登录系统，销毁所有时间戳（包括备份），检测能否销毁成功；

c） 在 TSA 证书失效后，并且超过了规定的保存时间，以 TSA 管理员身份登录系统，销毁所有时间戳（包括备份），检测能否销毁成功。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.2.5 时间戳的查看和验证

4.6.2.5.1 时间戳的查看

评价内容：

见 GB/T 20520—2006 中 7.5.1 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳的查看进行说明。

测试评价指南：

通过 TSA 提供的查看时间戳的方法，检测用户能否查看时间戳中所有可查看的内容。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.2.5.2 时间戳的验证

评价内容：

见 GB/T 20520—2006 中 7.5.2 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳的验证进行说明。

测试评价指南：

a） 通过 CRL 或 OCSP 协议，检测用户能否验证 TSA 证书的有效性；

b） 通过 TSA 提供的验证时间戳的方法，检测用户能否验证时间戳是由该 TSA 签发；

c) 通过 TSA 提供的验证时间戳的方法，检测用户能否验证时间戳是指定文件的时间戳。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3 时间戳的格式

4.6.3.1 对 TSA 的要求

评价内容：

见 GB/T 20520—2006 中 8.1 的内容。

对开发者的要求：

开发者应提供文档，针对 TSA 系统进行说明。

测试评价指南：

a) 检测所颁发的时间戳里，是否包含以下内容：

1) 一个可信时间值；

2) 一个一次性随机整数(nonce 域)；

3) 一个唯一的标识符(表明了时间戳生成时的安全策略)。

b) 检测 TSA 能否检查单向散列函数的标识符，能否验证散列值长度的正确性。

c) 检测是否只在散列值上盖时间戳。

d) 检测时间戳内是否包含任何请求方的标识，如果包含，则此项不符合。

e) 检测 TSA 系统是否使用专门的密钥对时间戳签名，并检测密钥对应证书中是否说明了该密钥的这个用途。

f) 使请求方在申请消息的扩展域内提出一些额外的要求，如果 TSA 支持这些扩展，检测时间戳内是否包含相应的扩展信息。

g) 使请求方在申请消息的扩展域内提出一些额外的要求，如果 TSA 不支持这些扩展，检测 TSA 是否返回一个出错信息。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.2 密钥标识

评价内容：

见 GB/T 20520—2006 中 8.2 的内容。

对开发者的要求：

开发者应提供文档，针对密钥标识进行说明。

测试评价指南：

检测 TSA 系统的所有密钥对应的证书中，是否包含唯一的 Key Usage 扩展域，并检测格式是否正确。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.3 时间的表示格式

评价内容：

见 GB/T 20520—2006 中 8.3 的内容。

对开发者的要求：

开发者应提供文档，针对时间的表示格式进行说明。

测试评价指南：

检测时间戳的时间表示格式是否正确。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.4 时间戳申请和响应消息格式

4.6.3.4.1 申请消息格式

评价内容：

见 GB/T 20520—2006 中 8.4.1 的内容。

对开发者的要求：

开发者应提供文档，针对申请消息格式进行说明。

测试评价指南：

检测时间戳的申请消息格式是否正确。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.4.2 响应消息格式

评价内容：

见 GB/T 20520—2006 中 8.4.2 的内容。

对开发者的要求：

开发者应提供文档，针对响应消息格式进行说明。

测试评价指南：

检测时间戳的响应消息格式是否正确。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.5 保存文件

评价内容：

见 GB/T 20520—2006 中 8.5 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳申请和响应消息的文件保存格式进行说明。

测试评价指南：

a) 将时间戳申请消息保存为文件，检测文件扩展名是否为：tsg；使用二进制查看工具查看文件是否只包含消息的 DER 编码，并检测编码格式是否正确；

b) 将时间戳响应消息保存为文件，检测文件扩展名是否为：tsr；使用二进制查看工具查看文件是否只包含消息的 DER 编码，并检测编码格式是否正确。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.6 所用 MIME 对象定义

4.6.3.6.1 电子邮件传输

评价内容：

见 GB/T 20520—2006 中 8.6.1 的内容。

对开发者的要求：

开发者应提供文档，针对电子邮件传输格式进行说明。

测试评价指南：

a) 如果使用电子邮件传输时间戳申请和响应消息，则本项为检测项目，否则为非检测项；

b) 使用电子邮件进行时间戳申请，并获取时间戳；

c) 使用协议分析仪截取整个时间戳申请和响应的数据包，并进行协议还原，检测时间戳申请和响应消息的格式是否符合标准。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.6.2 HTTP 传输

评价内容：

见 GB/T 20520—2006 中 8.6.2 的内容。

对开发者的要求：

开发者应提供文档，针对 HTTP 传输格式进行说明。

测试评价指南：

a) 如果使用 HTTP 协议传输时间戳申请和响应消息，则本项为检测项目，否则为非检测项；

b) 使用 HTTP 协议进行时间戳申请，并获取时间戳；

c) 使用协议分析仪截取整个时间戳申请和响应的数据包，并进行协议还原，检测时间戳申请和响应消息的格式是否符合标准。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.3.7 时间戳格式的安全考虑

评价内容：

见 GB/T 20520—2006 中 8.7 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳格式的安全考虑进行说明。

测试评价指南：

a) 检测请求方在产生 nonce 时，是否使用一次性随机数；

b) 检测请求方是否不采用局部时钟来考虑等待响应的时间；

c) 分别以不同实体身份用同样的数据和同样的散列算法申请时间戳，检测 TSA 系统的处理措施是否正确；

d) 以同一实体身份对同一对象多次申请时间戳，检测 TSA 系统和客户端的处理措施是否正确；

e) 检测 TSA 系统是否采用 nonce 域申请消息，以检查重放攻击；

f) 检测 TSA 系统是否采用局部时钟和移动的时间窗口，以检查重放攻击。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.4 时间戳系统的安全

4.6.4.1 可信时间源

评价内容：

见 GB/T 20520—2006 中 9.2.2 的内容。

对开发者的要求：

开发者应提供文档，针对时间戳的完整性保护措施进行说明。

测试评价指南：

a) 通过协议分析仪截取可信时间传输的网络数据包，检测是否采取完整性保护措施；

b) 篡改时间信息，检测签名系统能否发现时间信息已被篡改，检测能否向 TSA 管理者发出警报。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.4.2 审计

4.6.4.2.1 审计数据产生

评价内容：

见 GB/T 20520—2006 中 9.2.5.1 的内容。

对开发者的要求：

开发者应提供文档，针对审计事件进行说明。

测试评价指南：

a) 检测 TSA 的签名系统是否对以下事件产生审计记录：

1) 审计功能的启动和结束；

2) 表 1 中的事件。

表 1 审计事件

TSA 功能	事 件	附加信息
安全审计	所有对审计变量（如：时间间隔，审计事件的类型）的改变	
	所有删除审计记录的企图	
	对审计日志签名	数字签名，散列结果或认证码应该保存在审计日志之中
本地数据输入	所有的安全相关数据输入系统	若输入的数据与其他数据相关则须验证用户访问相关数据的权限
远程数据输入	所有被系统所接受的安全相关信息	
数据输出	所有对关键的或安全相关的信息进行输出的请求	
私钥载入	部件私钥的载入	
私钥的存储	对为私钥恢复而保存的证书主体私钥读取	
可信公钥的输入，删除和存储	所有对于可信公钥的改变（如：添加、删除）	包括公钥和与公钥相关的信息

表 1（续）

TSA 功能	事　件	附加信息
私钥和对称密钥的输出	私钥和对称密钥（包括一次性会话密钥）的输出	
时间戳申请	所有的时间戳申请请求	若申请成功，在日志中保存申请请求和产生的时间戳的拷贝； 若申请失败，在日志中保存失败原因和产生的时间戳失败响应的拷贝
部件的配置	所有的与安全相关的配置	
可信时间的获取和同步	根据可信时间源同步时间	包括如果可信时间和本地时间不匹配时，根据可信时间改变本地时间，以及同步过程中发生的所有错误

b）　对于表 1 中的每一个事件，检测审计记录是否包括以下内容：事件的日期和时间、用户、事件类型、事件是否成功，表中附加信息栏中要求的内容。

c）　检测日志记录中是否出现以下内容：明文形式的私钥、非对称密钥和其他安全相关的参数，如果出现，则此项不符合。

d）　检测每个可审计事件是否与发起该事件的系统用户身份关联。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.4.2.2　审计查阅

评价内容：

见 GB/T 20520—2006 中 9.2.5.2 的内容。

对开发者的要求：

开发者应提供文档，针对审计查阅进行说明。

测试评价指南：

a）　以审计员身份登录系统，尝试对审计记录进行查阅，检测是否成功查看日志信息；

b）　查看日志信息的内容是否为人所理解。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.4.2.3　审计事件存储

评价内容：

见 GB/T 20520—2006 中 9.2.5.3 的内容。

对开发者的要求：

开发者应提供文档，针对审计事件存储进行说明。

测试评价指南：

a）　尝试对审计记录进行非授权的修改，检测能否修改成功，能否检测出对审计记录的修改；

b）　产生大量审计记录，直至审计存储已满，检测审计功能部件能否阻止所有审计事件的发生（除非该事件是由审计员发起的）。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.4.2.4 可信的时间

评价内容：

见 GB/T 20520—2006 中 9.2.5.4 的内容。

对开发者的要求：

开发者应提供文档，针对审计记录的可信时间进行说明。

测试评价指南：

检测每条审计记录是否都有时间，并且检测审计记录的时间是否来源于可信时间源。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

4.6.4.2.5 审计日志签名

评价内容：

见 GB/T 20520—2006 中 9.2.5.5 的内容。

对开发者的要求：

开发者应提供文档，针对进行说明。

测试评价指南：

a) 检测 TSA 能否定期给审计日志加盖时间戳，并检测时间周期是否可配置；

b) 检测时间戳签名的对象是否为上次生成时间戳后加入的所有审计日志条目以及上次签名的时间戳的值；

c) 检测是否对加盖时间戳的事件进行审计，并检测审计记录中是否包含时间戳。

记录测试结果并对该结果是否完全符合上述测试评价指南要求作出判断。

如果以上结果全部正确，则本项满足。

5 综合评价

对公钥基础设施各测试项目的综合评价，见表 2 综合评价表。

表 2 综合评价表

测试项目	序号	测试子项目	综合评价
在线证书状态协议测试评价指南	4.1.1	总则	如果系统提供了在线证书状态查询功能，每一个子项目都满足相关要求，则系统满足 GB/T 19713—2005 的相关要求
	4.1.2	功能要求	
	4.1.3	安全考虑	
证书管理协议测试评价指南	4.2.1	必需的 PKI 管理功能	每一个子项目都满足相关要求，则系统满足 GB/T 19714—2005 的相关要求
	4.2.2	传输	
	4.2.3	必选的 PKI 管理消息结构	
PKI 组件最小互操作规范测试评价指南	4.3.1	PKI 组件规范	每一个子项目都满足相关要求，则系统满足 GB/T 19771—2005 的相关要求
	4.3.2	数据格式	

表 2（续）

测试项目	序号	测试子项目	综合评价
数字证书格式测试评价指南	4.4.1	基本证书域的数据结构	每一个子项目都满足相关要求，则系统满足 GB/T 20518—2006 的相关要求
	4.4.2	TBSCertificate 及其数据结构	
	4.4.3	证书扩展项	此子项目不作为判断系统是否满足的条件
特定权限管理中心技术规范测试评价指南	4.5.1	系统相关协议	如果系统提供了特定权限管理中心功能，每一个子项目都满足相关要求，则系统满足 GB/T 20519—2006 的相关要求
	4.5.2	PMI/AA 的安全实施	
	4.5.3	属性证书格式	
时间戳规范测试评价指南	4.6.1	时间戳的产生和颁发	如果系统提供了时间戳功能，每一个子项目都满足相关要求，则系统满足 GB/T 20520—2006 的相关要求
	4.6.2	时间戳的管理	
	4.6.3	时间戳的格式	
	4.6.4	时间戳系统的安全	

所有测试项目的汇总表参见附录 A 中的表 A.1 测试项目总表。

6 公钥基础设施测试环境示例

一个最基本的公钥基础设施一般由以下五个组件组成：

a） CA 负责生成、撤销、公布和存档证书的权威机构；

b） RA 是为用户办理证书申请、身份审核、证书下载、证书更新、证书注销以及密钥恢复等实际业务的办事机构或业务受理点；

c） 终端实体是不以签署证书为目的而使用其私钥的证书主体或者是依赖（证书）方；

d） 证书资料库存储证书和 CRL 等信息的数据库，并提供无需验证的信息检索服务；

e） 密码服务器是生成、存储密钥对并进行密码运算的专门设备。

此外，一个完整的 PKI 系统还可能包括时间戳服务器、特定权限管理中心、在线证书状态查询模块等。不同的 PKI 系统包含的组件不同，因此结构也不同。

图 1 给出了公钥基础设施测试环境网络结构图的一个示例。在实际的测试评价活动中，评价者应根据开发者提供的文档和组件搭建合适的测试环境。

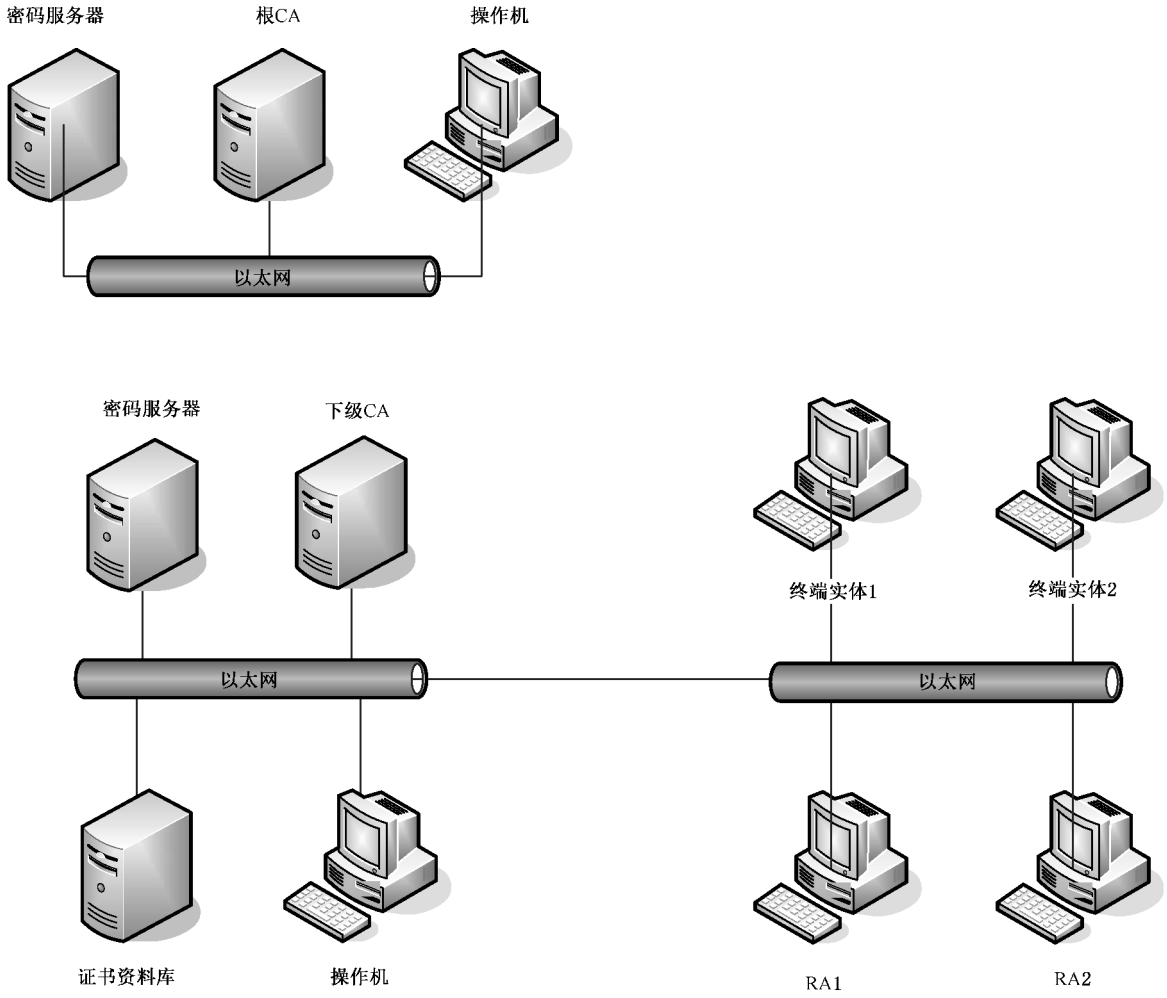

图 1　测试环境网络结构图

附 录 A
（资料性附录）
测试项目总表

所有测试项目的汇总参见表 A.1。

表 A.1 测试项目总表

序号	测试项目			
1	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	
2			4.1.1.2 响应	
3			4.1.1.3 异常情况	
4			4.1.1.4 thisUpdate、nextUpdate 和 producedAt 的语义	
5			4.1.1.5 OCSP 签名机构的委托	
6			4.1.1.6 CA 密钥泄露	
7		4.1.2 功能要求	4.1.2.1 证书内容	
8			4.1.2.2 签名响应的接收要求	
9			4.1.3 安全考虑	
10	4.2 证书管理协议测试评价指南	4.2.1 必需的 PKI 管理功能	4.2.1.1 根 CA 初始化	
11			4.2.1.2 根 CA 密钥更新	
12			4.2.1.3 下级 CA 初始化	
13			4.2.1.4 CRL 产生	
14			4.2.1.5 PKI 信息请求	
15			4.2.1.6 交叉认证	
16			4.2.1.7 终端实体初始化	4.2.1.7.1 获得 PKI 信息
17				4.2.1.7.2 根 CA 密钥的带外验证
18			4.2.1.8 证书请求	
19			4.2.1.9 密钥更新	
20		4.2.2 传输		
21		4.2.3 必选的 PKI 管理消息结构	4.2.3.1 初始的注册/认证（基本认证方案）	
22			4.2.3.2 证书请求	
23			4.2.3.3 密钥更新请求	
24	4.3 PKI 组件最小互操作规范测试评价指南	4.3.1 PKI 组件规范	4.3.1.1 证书认证机构（CA）	4.3.1.1.1 颁发数字签名证书
25				4.3.1.1.2 颁发加密证书
26				4.3.1.1.3 交叉认证
27				4.3.1.1.4 撤销证书
28				4.3.1.1.5 请求 CA 证书
29			4.3.1.2 注册机构（RA）	

表 A.1（续）

序号	测试项目			
30	4.3 PKI 组件最小互操作规范测试评价指南	4.3.1 PKI 组件规范	4.3.1.3 证书持有者规范	
31			4.3.1.4 客户规范	
32		4.3.2 数据格式	4.3.2.1 证书撤销列表	
33			4.3.2.2 事务消息格式	4.3.2.2.1 全体 PKI 消息组件
34				4.3.2.2.2 通用数据结构
35				4.3.2.2.3 特殊操作的数据结构
36			4.3.2.3 PKI 事务	4.3.2.3.1 RA 发起的注册请求
37				4.3.2.3.2 新实体的自我注册请求
38				4.3.2.3.3 已知实体的自我注册请求
39				4.3.2.3.4 证书更新
40				4.3.2.3.5 PKCS＃10 自我注册请求
41				4.3.2.3.6 撤销请求
42				4.3.2.3.7 集中产生密钥对和密钥管理证书申请
43				4.3.2.3.8 组合证书申请
44	4.4 数字证书格式测试评价指南	4.4.1 基本证书域的数据结构		
45		4.4.2 TBSCertificate 及其数据结构	4.4.2.1 版本 version	
46			4.4.2.2 序列号 serial number	
47			4.4.2.3 签名算法 signature	
48			4.4.2.4 颁发者 issuer	
49			4.4.2.5 有效期 validity	
50			4.4.2.6 主体 subject	
51			4.4.2.7 主体公钥信息 Subject Public Key Info	
52			4.4.2.8 颁发者唯一标识符 IssuerUniqueID	
53			4.4.2.9 主体唯一标识符 SubjectUniqueID	
54		4.4.3 证书扩展项	4.4.3.1 标准扩展	
55			4.4.3.2 专用因特网扩展	
56	4.5 特定权限管理中心技术规范测试评价指南	4.5.1 系统相关协议	4.5.1.1 代理点 PA 与属性注册机构 ARA 间的通信协议	4.5.1.1.1 功能支持
57				4.5.1.1.2 PA 与 ARA 之间的认证机制
58				4.5.1.1.3 PA 数据签名
59			4.5.1.2 属性注册机构 ARA 与属性授权机构 AA 间的通信协议	
60			4.5.1.3 属性授权机构 AA 与认证机构源 SOA 间的通信协议	
61		4.5.2 PMI/AA 的安全实施	4.5.2.1 证书撤销安全	
62			4.5.2.2 算法强度安全	
63			4.5.2.3 身份标识安全	
64			4.5.2.4 LDAP 服务访问安全	
65			4.5.2.5 属性内容安全	
66		4.5.3 属性证书格式		

表 A.1（续）

序号	测试项目			
67	4.6 时间戳规范测试评价指南	4.6.1 时间戳的产生和颁发	4.6.1.1 申请和颁发方式	
68			4.6.1.2 可信时间的产生方法	
69			4.6.1.3 时间的同步	
70			4.6.1.4 申请和颁发过程	
71		4.6.2 时间戳的管理	4.6.2.1 时间戳的保存	4.6.2.1.1 在 TSA 方的保存
72				4.6.2.1.2 在用户方的保存
73			4.6.2.2 时间戳的备份	
74			4.6.2.3 时间戳的检索	
75			4.6.2.4 时间戳的删除和销毁	4.6.2.4.1 时间戳的删除
76				4.6.2.4.2 时间戳的销毁
77			4.6.2.5 时间戳的查看和验证	4.6.2.5.1 时间戳的查看
78				4.6.2.5.2 时间戳的验证
79		4.6.3 时间戳的格式	4.6.3.1 对 TSA 的要求	
80			4.6.3.2 密钥标识	
81			4.6.3.3 时间的表示格式	
82			4.6.3.4 时间戳申请和响应消息格式	4.6.3.4.1 申请消息格式
83				4.6.3.4.2 响应消息格式
84			4.6.3.5 保存文件	
85			4.6.3.6 所用 MIME 对象定义	4.6.3.6.1 电子邮件传输
86				4.6.3.6.2 HTTP 传输
87			4.6.3.7 时间戳格式的安全考虑	
88		4.6.4 时间戳系统的安全	4.6.4.1 可信时间源	
89			4.6.4.2 审计	4.6.4.2.1 审计数据产生
90				4.6.4.2.2 审计查阅
91				4.6.4.2.3 审计事件存储
92				4.6.4.2.4 可信的时间
93				4.6.4.2.5 审计日志签名

中 华 人 民 共 和 国
国 家 标 准
信息安全技术 公钥基础设施
标准一致性测试评价指南
GB/T 30272—2013
*
中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014年5月第一版
*
书号:155066·1-49176

GB/T 30272-2013