ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 21054—XXXX

信息安全技术 公钥基础设施 PKI 系统安全测评方法

Information security technques—Public key infrastructure—Security testing assessment approaches for PKI system

（征求意见稿）

（本稿完成日期：2021 年 8 月 6 日）

在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。

XXXX－　－XX 发布　　XXXX－　－XX 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

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 21054-2007《信息安全技术 公钥基础设施 PKI 系统安全等级保护评估准则》。与 GB/T 21053-2007 相比，除结构调整和编辑性改动外，主要技术变化如下：

将名称修改为《信息安全技术 公钥基础设施 PKI 系统安全测评方法》，本文件依据 GB/T 21053 规定的 PKI 系统产品的等级及相应等级的安全技术要求，给出了对应的测评方法。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出并归口。

本文件起草单位：中国科学院软件研究所、中国科学院大学、公安部第三研究所、成都卫士通信息产业股份有限公司、北京信安世纪科技有限公司、北京数字认证股份有限公司、长春吉大正元信息技术股份有限公司、北京百度网讯科技有限公司、北京奇虎科技有限公司、北京软件产品质量检测检验中心、格尔软件股份有限公司、国网区块链科技（北京）有限公司、华为技术有限公司、天津南大通用数据技术股份有限公司、同智伟业软件股份有限公司、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）、中国汽车工程研究院股份有限公司、中国信息通信研究院、中金金融认证中心有限公司。

本文件主要起草人：张严、张立武、顾健、陈妍、邱梓华、刘丽敏、张立廷、汪宗斌、傅大鹏、王榕、李健、郑强、张屹、董晶晶。

本文件及其所替代的文件的历次版本发布情况为：

——GB/T 21054-2007。

信息安全技术 公钥基础设施 PKI 系统安全测评方法

1 范围

本文件依据GB/T 21053-XXXX规定了PKI系统的安全测评方法。

本文件适用于 PKI 系统产品的测试和评估，对于 PKI 系统安全功能的研制、开发、测试和产品采购亦可参照使用。

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，仅所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 20271-2006 信息安全技术 信息系统通用安全技术要求

GB/T 20518-2018 信息安全技术 公钥基础设施 数字证书格式

GB/T 20984-2007 信息安全技术 信息安全风险评估规范

GB/T 21052-2007 信息安全技术 信息系统物理安全技术要求

GB/T 21053 信息安全技术 公钥基础设施 PKI 系统安全技术要求

GB/T 25056-2018 信息安全技术 证书认证系统密码及其相关安全技术规范

GM/T 0014-2012 数字证书认证系统密码协议规范

3 术语和定义

GB/T 21053中规定的术语适用于本文件。

4 缩略语

下列缩略语适用于本文件。

CA：认证机构(Certification Authority)

CRL：证书撤销列表(Certificate Revocation List)

OCSP：在线证书状态协议(Online Certificate Status Protocol)

RA：注册机构(Registration Authority)

5 概述

在进行评估前，应提出待评估PKI系统的拟定安全等级，然后依据本文件6章至7章中的测评流程，对照GB/T 21053-XXXX中的安全技术要求进行评估。对于每一个安全要素，如果评估流程的执行结果与预期结果一致，则判定为符合，否则判定为不符合。当所有安全要素的评估结束后，根据结果给出待评估PKI系统的安全等级；

6 基本级安全测评方法

6.1 安全功能测评方法

6.1.1 通用密钥管理

6.1.1.1 密钥导入导出

密钥导入导出部分的测评方法如下：

a) 测评流程：

1) 结合文档和对实际系统的分析，确定密钥导入导出时是否采用国家密码行政管理部门认可的加密算法或加密设备；
2) 结合文档和对实际系统的分析，确定各类私钥的导入导出流程，确认导入导出过程中，密钥是否始终以加密形式存在；
3) 确认 PKI 系统是否具有将导入导出密钥与实体关联和赋予权限的机制，例如：在导入密钥时，要求输入密钥的所有者信息、在系统中维护密钥索引与用户实体的映射列表、针对导入导出密钥的权限分配列表等等；
4) 通过尝试访问登录实体无权限使用的密钥等方式，确定 PKI 系统是否实现了对导入导出密钥的管理。

b) 预期结果：

1) PKI 系统密钥的实际导入导出方法与文档中的规定一致；
2) PKI 系统的各类私钥不应以明文形式导入导出 PKI 系统；
3) 各类私钥的导入导出过程中，密钥始终以加密形式存在；
4) PKI 系统提供了将导入导出密钥与实体关联并赋予权限的机制；
5) 对于与导入导出密钥赋予权限不匹配的密钥操作，PKI 系统拒绝执行。

6.1.2 PKI 系统密钥管理

6.1.2.1 PKI 系统密钥生成

PKI 系统密钥生成部分的测评方法如下：

a) 测评流程：

确定 PKI 系统在密钥生成时应检查用户角色，并设置为只有管理员才能启动 CA 密钥生成过程。

b) 预期结果：

只有管理员才能执行 PKI 系统的 CA 密钥生成过程；

6.1.2.2 PKI 系统密钥传送与分发

PKI 系统密钥传送与分发部分的测评方法如下：

a) 测评流程：

1) 结合文档等确定 PKI 系统中部件密钥、系统用户密钥、CA 密钥等各类系统密钥的传送与分发方法；
2) 结合文档和对实际传递消息的分析，确定 CA 公钥分发方法是否具有可行性，是否对 CA 公钥应用了数字签名或消息鉴别码等完整性保护机制；
3) 确定 PKI 系统文档中是否明确规定了 CA 密钥分发方法；包括：CA 密钥传送过程的参与方、具体的流程、使用的完整性保护机制和加密机制等。

b) 预期结果：

1) 能够确定 PKI 系统中部件密钥、系统用户密钥、CA 密钥和终端用户密钥等各类密钥的传送与分发方法；实际的传送和分发方法与文档中的规定一致；
2) CA 公钥分发方法具有可行性，对 CA 公钥进行了完整性保护；
3) PKI 系统文档中明确规定了 CA 密钥分发方法。

6.1.2.3 PKI 系统密钥存储

PKI 系统密钥存储部分的测评方法如下：

a) 测评流程：

1) 结合文档和对实际存储介质的分析，确定 PKI 系统部件密钥和系统用户密钥的存储方式是否为以下方式之一：存储于密码模块中；以加密的形式存储；
2) 当使用密码模块时，确定密码模块是否符合国家密码行政管理部门规定；当使用加密形式存储时，确定对加密密钥的管理方式是否存在可能的安全风险，包括：在存储介质中以明文形式保存加密密钥、在代码中写入明文形式的加密密钥等等。

b) 预期结果：

1) PKI 系统部件密钥和系统用户密钥存储于国家密码行政管理部门规定密码模块中；以加密的形式存储；对加密密钥进行了安全管理。

6.1.3 用户密钥管理

6.1.3.1 终端用户密钥传送与分发

终端用户密钥传送与分发部分的测评方法如下：

a) 测评流程：

1) 结合文档等确定终端用户密钥等各类密钥的传送与分发方法；
2) 确定终端用户的密钥生成方式；如果终端用户自己生成密钥对，确定终端用户向 PKI 系统提交用户公钥的流程中，是否对用户公钥应用了数字签名或消息鉴别码等完整性保护机制；如果终端用户委托 CA 生成密钥对，确定 CA 向用户传送与分发私钥时，是否对用户私钥进行了加密，确定加密密钥的生成方式；。上述过程应结合文档和对实际传递消息的分析进行。

b) 预期结果：

1) 能够确定 PKI 系统中终端用户密钥等各类密钥的传送与分发方法；实际的传送和分发方法与文档中的规定一致；
2) 终端用户自己生成密钥对时，终端用户向 PKI 系统提交用户公钥的流程中，对用户公钥进行了完整性保护；
3) 终端用户委托 CA 生成密钥对时，CA 向用户传送与分发私钥时，对用户私钥进行了加密；加密密钥的生成采用了密钥协商等安全方法。

6.1.4 轮廓管理

6.1.4.1 证书轮廓管理

证书轮廓管理部分的测评方法如下：

a) 测评流程：

1) 根据文档，确定 PKI 系统是否具有证书轮廓；
2) 验证证书轮廓中的信息，确定证书轮廓中所定义的字段和扩展是否均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 确定证书轮廓中是否包含以下所有信息：

——与密钥绑定的用户的标识符；
——主体的公私密钥对可使用的加密算法；
——证书发布者的标识符；
——证书有效时间的限定；
——证书包括的附加信息；
——证书的主体是否是 CA；
——与证书相对应的私钥可执行的操作；
——证书发布所使用的策略。

4) 确定证书轮廓中，是否为所有以下字段和扩展指定了可能的取值：
——密钥所有者的标识符；
——公私密钥对主体的算法标识符；
——证书发布者的标识符；
——证书的有效期。
——keyUsage；
——basicConstraints；
——certificatePolicies；

5) 对比 PKI 系统颁发的证书，确定所有证书的内容是否与证书轮廓一致。

b) 预期结果：

1) PKI 系统具有证书轮廓；
2) 证书轮廓中所定义的字段和扩展均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 证书轮廓中包含所列出的各项信息；
4) 证书轮廓中为列出的所有字段和扩展指定了可能的取值；
5) 进行验证的所有证书的内容与证书轮廓一致。

6.1.4.2 证书撤销列表轮廓管理

证书撤销列表轮廓管理部分的测评方法如下：

a) 测评流程：

1) 根据文档，确定 PKI 系统是否发布 CRL，如果发布 CRL，PKI 系统是否具有证书撤销列表轮廓；
2) 验证证书撤销列表轮廓中的信息，确定证书撤销列表轮廓中所定义的字段和扩展是否均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 确定证书轮廓中，是否为所有以下字段和扩展指定了可能的取值：
——issuer;
——issuerAltName；
——NextUpdate。
4) 对比 PKI 系统颁发的 CRL，确定所有 CRL 的内容是否与证书撤销列表轮廓一致。

b) 预期结果：

1) 如果 PKI 系统发布 CRL，PKI 系统具有证书撤销列表轮廓；
2) 证书撤销列表轮廓中所定义的字段和扩展均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 证书撤销列表轮廓中包含所列出的各项信息；
4) 进行验证的所有 CRL 的内容与证书撤销列表轮廓一致。

6.1.4.3 在线证书状态协议轮廓管理

OCSP 轮廓管理部分的测评方法如下：

a) 测评流程：

1) 根据文档，确定 PKI 系统是否发布 OCSP 响应，如果发布 OCSP 响应，PKI 系统是否具有在线证书状态协议轮廓；
2) 确定在线证书状态协议轮廓中，是否为 responseType 字段指定了可接受的值；
3) 若 PKI 系统允许使用基本相应类型（basic response type）的 OCSP 响应，确定在线证书状态协议轮廓中，是否为 ResponseID 字段指定了可接受的值；
4) 结合文档，构建测试用 OCSP 请求，将 OCSP 请求发送至 PKI 系统的 OCSP 服务并记录返回的消息，确认该消息与在线证书状态协议轮廓中的描述一致。

b) 预期结果：

1) 如果 PKI 系统发布 OCSP 响应，PKI 系统具有在线证书状态协议轮廓；
2) 在线证书撤销列表轮廓中为 responseType 指定了可能的取值；
3) 若 PKI 系统允许使用基本相应类型，在线证书状态协议轮廓中为 ResponseID 字段指定了可接受的值；
4) 进行验证获取的所有 OCSP 响应的内容与在线证书状态协议轮廓一致。

6.1.5 证书管理

6.1.5.1 证书注册

证书注册部分的测评方法如下：

a) 测评流程：

1) 生成测试证书请求，提交至 PKI 系统执行证书注册流程，确定 PKI 系统是否对输入证书字段和扩展中的数据进行了批准，确定 PKI 系统对证书数据的批准方式；
2) 检查通过测试证书注册流程获取的证书，确定其格式是否符合 GB/T 20518-2018 的要求；
3) 结合 PKI 系统的证书轮廓检查通过测试证书注册流程获取的证书，确定颁发的证书是否与证书轮廓中定义相符；
4) 若 PKI 系统允许用户密钥对由用户生成，则执行证书请求，选择由用户生成密钥对，然后使用不知道对应私钥作为证书请求的公钥，确定 PKI 系统是否对证书主体拥有与证书中包含的公钥相对应的私钥；
5) 检查通过测试证书注册流程获取的证书，确定其内容是否符合以下要求：

——version 字段应为 0,1,2；
——若包含 issuerUniqueID 或 subjectUniqueID 字段，则 version 字段应为 1 或 2；
——若证书包含 extensions，那么 version 字段应为 2；
——serialNumber 字段对 CA 应是唯一的；
——validity 字段应说明不早于当时时间的 notBefore 值和不早于 notBefore 时间的 notAfter 值；
——若 issuer 字段为空，证书应包括一个 issuerAltName 的关键性扩展；
——若 subject 字段为空，证书应包括一个 subjectAltName 的关键性扩展；
——subjectPublicKeyInfo 字段中的 signature 字段和 algorithm 字段应包含国家密码行政管理部门许可的或推荐的算法的 OID。

b) 预期结果：

1) PKI 系统的证书注册流程中包含对输入证书字段和扩展中的数据进行批准的操作，批准方式为以下方式之一：

——数据被操作员手工批准；

——自动过程检查和批准数据；
——字段或扩展的值由 PKI 系统自动生成；
——字段或扩展的值从证书轮廓中获得。

2) 当方式为手工批准或自动检查和批准时，不符合要求的数据不会被批准；
3) 若 PKI 系统允许用户密钥对由用户生成，则 PKI 系统对证书主体拥有与证书中包含的公钥相对应的私钥，不持有与公钥对应的私钥情况下，证书注册请求无法完成；
4) 通过测试证书注册流程获取的证书，其内容符合本节中的要求。

6.1.5.2 证书撤销

6.1.5.2.1 证书撤销列表审核

证书撤销列表审核部分的测评方法如下：

a) 测评流程：

确定 PKI 系统是否发布 CRL，如果发布，则执行以下流程：

1) 结合文档与对实际系统的分析，确定 PKI 系统是否实现了证书撤销列表审核机制；
2) 确认证书撤销列表审核机制是否验证 CRL 的所有强制性字段的值符合 GB/T 20518-2018。并实现了对以下内容的检查：

——若包含 version 字段，应为 1；
——若 CRL 包含关键性的扩展，version 字段应出现且为 1；
——signature 和 signatureAlgorithm 字段应为许可的数字签名算法的 OID；
——thisUpdate 应包含本次 CRL 的发布时间；
——nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

3) 查看 PKI 系统发布的 CRL，确认发布的 CRL 的内容是否与规定的证书撤销列表审核机制一致。

a) 预期结果：

如果 PKI 系统发布 CRL，则按照以下预期结果进行确认：

1) PKI 系统实现了证书撤销列表审核机制；
2) 证书撤销列表审核机制验证 CRL 的所有强制性字段的值符合 GB/T 20518-2018。并实现了对相关内容的检查；
3) 发布的 CRL 的内容与规定的证书撤销列表审核机制一致。

6.1.5.2.2 OCSP 基本响应的审核

OCSP 基本响应审核部分的测评方法如下：

a) 测评流程：

确定 PKI 系统是否发布 OCSP 响应，如果发布，则执行以下流程：

1) 结合文档与对实际系统的分析，确定 PKI 系统是否实现了 OCSP 基本响应审核机制；
2) 确认 OCSP 基本响应审核机制是否验证所有强制性字段的值符合 GB/T 17913-2005；
3) 确认 OCSP 基本响应审核机制是否实现了对以下内容的检查：

——Version 字段应为 0；
——signatureAlgorithm 字段应为许可的数字签名算法的 OID；
——thisUpdate 字段应指出证书状态正确的时间；
——producedAt 字段应指出 OCSP 响应者发出响应的时间；
——nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

4) 查看 PKI 系统发布的 OCSP 响应，确认发布的 OCSP 响应的内容是否与规定的 OCSP 基本响应审核机制一致。

b) 预期结果：

如果 PKI 系统发布 OCSP 响应，则按照以下预期结果进行确认：

1) PKI 系统实现了 OCSP 基本响应审核机制审核机制；
2) OCSP 基本响应审核机制验证所有强制性字段的值符合 GB/T 17913-2005；
3) OCSP 基本响应审核机制实现了对相关内容的检查；
4) 发布的 OCSP 响应的内容与规定的 OCSP 基本响应审核机制一致。

6.1.6 身份鉴别

6.1.6.1 用户属性定义

用户属性定义部分的测评方法如下：

a) 测评流程：

确定 PKI 系统是否维护用户属性定义，即对于每个用户，给出该用户所具有的属性信息，维护属性定义的方式包括：将属性定义记录在用户数据库中、为用户颁发属性证书等等；

b) 预期结果：

PKI系统提供了相应机制维护用户属性定义；

6.1.6.2 用户身份鉴别

用户鉴别部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统提供了相应机制，是否定义了在标识用户前可以由 PKI 系统代表用户执行的、与安全功能无关的动作，例如：响应查询公开信息；接收用户发来的数据，但直到系统用户批准之后才处理等等。确认这些事件的设置是否适当；
2) 在不进行鉴别的情况下，执行与安全无关的操作，确定操作能否被执行；
3) 在不进行鉴别的情况下，执行其它的安全功能引起的操作动作，确定操作能否被执行，是否要求用户进行鉴别；
4) 在进行鉴别的情况下，使用当前用户能够执行的安全功能引起的操作动作，确定操作能否被执行；
5) 在用户鉴别时，观察 PKI 系统的反馈，确定是否存在违反最小信息原则的或泄露用户的鉴别数据，例如：输入的口令被显示。

b) 预期结果：

1) PKI 系统设置了适当的在标识用户前可以由 PKI 系统代表用户执行的，这些操作与安全无关；
2) 在不进行鉴别的情况下，预先设置的、与安全无关的操作能够被执行；
3) 在不进行鉴别的情况下，执行其它的安全功能引起的操作动作时，PKI 系统要求用户进行鉴别，如果不进行鉴别，则操作不能够被执行；
4) 在进行鉴别的情况下，符合策略的安全功能引起的操作动作能够被执行；
5) 用户鉴别时 PKI 系统的反馈信息遵循最小信息原则，不包含用户鉴别信息。

6.1.6.3 鉴别失败处理

鉴别失败处理部分的测评方法如下：

a) 测评流程：

1) 执行 PKI 系统的鉴别操作，采用输入不正确的口令、提供不合法的用户证书等方式，执行失败的鉴别操作。确定 PKI 系统的安全功能是否能够检测到鉴别尝试不成功。
2) 结合 PKI 文档与相关配置信息，确定 PKI 系统是否设置了鉴别失败次数界限，然后对同一个用

户，重复执行 1）中的操作，直至尝试次数达到定义的界限，确定 PKI 系统是否能够检测到此事件的发生。

b) 预期结果：

1) 当进行不成功的鉴别尝试时，PKI 系统能够检测到该次鉴别不成功；
2) PKI 系统设置了鉴别失败次数界限；
3) 当达到预先设置的失败次数界限时，PKI 系统能够检测到此事件的发生。

6.1.7 访问控制

6.1.7.1 角色与责任

角色与责任部分的测评方法如下：

a) 测评流程：

1) 配置 PKI 系统；
2) 查看 PKI 系统使用文档，确定是否存在对系统管理员、操作员和**审计员**的角色定义；
3) 结合 PKI 文档对系统中的权限分配相关信息，包括：权限分配表、访问控制数据库、属性证书等进行分析，确定 PKI 系统中角色和权限的对应关系是否符合 GB/T 21053-XXXX 表 2；
4) 根据 GB/T 21053-XXXX 表 2 中所列出的操作，规划测试流程，测试流程应涵盖表#中所列出的所有操作，包括：安装、配置、维护系统；建立和管理用户账户；配置轮廓和审计参数；生成部件密钥；查看和维护审计日志；执行系统的备份和恢复；签发和撤销证书；
5) 使用具有系统管理员角色的主体登录系统，执行测试流程中所列出的所有操作；
6) 使用具有操作员角色的主体登录系统，执行测试流程中所列出的所有操作；
7) 验证 PKI 系统是否具有将主体与角色进行关联的能力；
8) 执行角色分配操作，尝试为测试主体分配系统管理员、操作员和审计员中的两个或更多数量的角色。

b) 预期结果：

1) PKI 系统开发者提供了对系统管理员、操作员和审计员的角色定义；
2) PKI 系统中角色和权限的对应关系符合 GB/T 21053-XXXX 表 5；
3) 当使用具有系统管理员角色的主体登录系统时，能够执行与系统管理员角色对应的所有操作，包括：安装、配置、维护系统；建立和管理用户账户；配置轮廓和审计参数；生成部件密钥；执行系统的备份和恢复。但对于其它操作，PKI 系统提示不具有相应权限；
4) 当使用具有操作员角色的主体登录系统时，能够执行与操作员角色对应的所有操作，包括：签发和撤销证书。但对于其它操作，PKI 系统提示不具有相应权限；
5) 当使用具有操作员角色的主体登录系统时，能够执行与操作员角色对应的所有操作，包括：查看和维护审计日志；但对于其它操作，PKI 系统提示不具有相应权限；
6) PKI 系统中应具有将主体与角色进行关联的能力；
7) 无法执行为测试主体分配系统管理员、操作员中的两个或更多数量角色的操作。

6.1.7.2 网络访问控制

网络访问控制部分的测评方法如下：

a) 测评流程：

1) 尝试通过网络对 PKI 系统服务进行访问，确定 PKI 系统对可能的路径提供了控制；
2) 使用远程计算机系统对 PKI 系统进行连接，确定是否需要进行认证；
3) 确定 PKI 系统是否提供了网络访问控制策略的定义；
4) 尝试访问 PKI 系统的诊断分析接口，确定是否需要进行认证，确定 PKI 系统是否对访问请求进

行了记录。

b) 预期结果：

1) PKI 系统对系统服务的访问请求进行了控制，无法直接访问这些系统服务；
2) PKI 系统对远程计算机的所有连接请求进行认证，认证不通过时，无法连接到 PKI 系统；
3) PKI 系统提供了网络访问控制策略的定义；
4) PKI 系统对诊断分析接口的所有访问请求进行认证，认证不通过时，无法访问诊断分析接口;
5) PKI 系统对诊断分析接口的所有访问请求进行记录，记录包括访问时间、请求方的 IP 地址，认证结果。

6.1.8 安全审计

6.1.8.1 审计数据产生

审计数据产生部分的测评方法如下：

a) 测评流程：

1) 结合 PKI 文档与相关配置信息，确定 PKI 系统是否提供了可审计事件维护功能；
2) 确定系统中已维护的所有可审计事件，确定 PKI 系统是否为每个审计事件生成了审计记录，审计记录中是否包含与审计事件相关的基本信息；
3) 选择性地与可审计事件相关的操作，然后查看审计记录，确定审计记录中记录了新发生的审计事件信息。

b) 预期结果：

1) PKI 系统提供了可审计事件维护功能，可以通过此功能对可审计事件进行维护；
2) PKI 系统为每个审计事件生成了审计记录，审计记录中包含与审计事件相关的基本信息；
3) 当执行与可审计事件相关的操作后，审计记录中能够增加新发生的审计事件信息。

6.1.8.2 审计查阅

审计查阅部分的测评方法如下：

a) 测评流程：

1) 结合 PKI 文档，确定 PKI 系统是否提供了审计记录查阅功能；
2) 确定审计查阅功能是否包含从审计记录中读取一定类型的审计信息的能力；
3) 选取若干审计信息类型，执行审计查阅，确定返回的审计记录与所选取的类型一致。

b) 预期结果：

1) PKI 系统是否提供了审计记录查阅功能；
2) 审计查阅功能包含从审计记录中读取一定类型的审计信息的能力；
3) 通过审计查阅功能，可以从审计记录中读取所选择类型的审计信息，返回的审计记录与所选取的类型一致。

6.1.8.3 选择性审计查阅

选择性审计部分的测评方法如下：

a) 测评流程：

1) 访问审计功能部件，结合 PKI 文档，确定审计功能部件是否提供了根据基本属性选择或排除审计事件集中的可审计事件的功能；
2) 执行可审计事件选择操作，选择和排除若干类型的可审计事件；
3) 选择性地与 2）中选择和排除的可审计事件相关的操作，然后查看审计记录，确定审计记录中是否记录了新发生的审计事件信息。

b) 预期结果：

1) 审计功能部件提供了根据基本属性选择或排除审计事件集中的可审计事件的功能；

2) 能够通过执行可审计事件选择操作，选择和排除特定类型的可审计事件；
3) 当选择某个类型的可审计事件后，执行与可审计事件相关的操作时，审计记录中能够增加新发生的审计事件信息；
4) 当排除某个类型的可审计事件后，执行与可审计事件相关的操作时，审计记录中不增加新发生的审计事件信息。

6.1.8.4 审计事件存储

审计事件存储部分的测评方法如下：

a) 测评流程：

1) 尝试以未授权形式对审计记录进行修改，例如：在不使用审计管理员进行鉴别的情况下，执行审计记录修改和删除操作；直接访问存储审计记录的数据库或文件，并进行修改；确定操作能否完成；
2) 尝试以授权形式对审计记录进行修改，例如：在使用审计管理员进行鉴别的情况下，执行审计记录修改操作；确定操作能否完成；
3) 确定审计功能部件是否提供了审计记录修改检测操作，在执行审计记录修改操作后，执行审计记录修改检测操作，确定审计功能部件能否检测到对审计记录的修改；
4) 将审计踪迹存储配置为已满状态，然后执行不由**审计员**发起的若干审计事件，确定审计功能部件是否阻止该事件的发生。

a) 预期结果：

1) 尝试以未授权形式对审计记录进行修改时，审计功能部件能够防止这些操作的执行，例如：执行操作时，提示权限不足；无法直接访问存储审计记录的数据库或文件等；
2) 尝试以授权形式对审计记录进行修改时，操作能够执行；
3) 审计功能部件提供了审计记录修改检测操作，执行审计记录修改检测操作，能够检测到对审计记录的修改，返回的修改记录与执行的修改操作一致；
4) 审计踪迹存储配置为已满状态时，审计功能部件应能够阻止由**审计员**发起的以外的所有审计事件的发生。

6.1.9 备份和恢复

备份与恢复部分的测评方法如下：

a) 测评流程：

1) 结合 PKI 文档，确定 PKI 系统是否提供了备份和恢复功能；
2) 尝试调用备份功能，确定在需要时是否能够调用备份功能生成系统备份数据；
3) 执行备份操作，然后对系统进行修改，然后尝试执行恢复功能，结合对备份数据的内容进行分析，确定是否能够通过系统备份数据重建备份时的系统状态。

b) 预期结果：

1) PKI 系统提供了备份和恢复功能；
2) 备份功能能够正常执行，执行备份操作后，能够生成当前时间节点的系统备份数据；
3) 系统备份数据中保存了足够的信息，能够通过执行恢复功能重建备份时的系统状态。

6.2 安全保障测评方法

6.2.1 开发

6.2.1.1 安全架构

安全架构部分的测评方法如下：

a) 测评流程：

1) 检查开发者提供的安全架构证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

2) 检查 PKI 系统与产品设计文档中对安全功能的描述范围是否相一致。

b) 预期结果：

开发者提供的信息应满足 GB/T 21053 6.2.1.1 中所述的要求。

6.2.1.2 功能规范

功能规范部分的测评方法如下：

a) 测评流程：

检查开发者提供的功能规范证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否清晰描述定义的产品安全功能;

2) 是否描述产品所有安全功能接口的目的、使用方法及相关参数;

3) 描述安全功能实施过程中,是否描述与安全功能接口相关的所有行为;

4) 是否描述可能由安全功能接口的调用而引起的所有直接错误消息。

b) 预期结果：

开发者提供的信息应满足 GB/T 21053 6.2.1.2 中所述的要求。

6.2.1.3 产品设计

产品设计部分的测评方法如下：

a) 测评流程：

检查开发者提供的产品设计证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否根据子系统描述产品结构,是否标识和描述产品安全功能的所有子系统,是否描述安全功能所有子系统间的相互作用；

2) 提供的对应关系是否能证实设计中描述的所有行为映射到调用的安全功能接口。

b) 预期结果：

开发者提供的信息应满足 GB/T 21053 6.2.1.3 中所述的要求。

6.2.2 指导性文档

6.2.2.1 操作用户指南

产品设计部分的测评方法如下：

a) 测评流程：

检查开发者提供的操作用户指南证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否描述用户能访问的功能和特权(包含适当的警示信息)；

2) 是否描述如何以安全的方式使用产品提供的可用接口,是否描述产品安全功能及接口的用户操作方法(包括配置参数的安全值);

3) 是否标识和描述产品运行的所有可能状态,包括操作导致的失败或者操作性错误；

4) 是否描述实现产品安全目的必需执行的安全策略。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.2.1中所述的要求。

6.2.2.2 准备程序

准备程序部分的测评方法如下：

a) 测评流程：

检查开发者提供的准备程序证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；
2) 是否描述安全安装产品及其运行环境必需的所有步骤。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.2.2中所述的要求。

6.2.3 生命周期支持

6.2.3.1 配置管理能力

配置管理能力部分的测评方法如下：

a) 测评流程：

检查开发者提供的配置管理能力证据,并检查开发者提供的信息是否满足内容和形式的所有要求:

1) 检查开发者是否为不同版本的产品提供唯一的标识；
2) 现场检查配置管理系统是否对所有的配置项作出唯一的标识,且是否对配置项进行了维护；
3) 检查开发者提供的配置管理文档,是否描述了对配置项进行唯一标识的方法。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.3.1中所述的要求。

6.2.3.2 配置管理范围

配置管理范围部分的测评方法如下：

a) 测评流程：

检查开发者提供的配置管理范围证据,并检查开发者提供的信息是否满足内容和形式的所有要求:

1) 检查开发者提供的配置项列表是否包含产品、安全保障要求的评估证据和产品的组成部分及相应的开发者。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.3.2中所述的要求。

6.2.3.3 交付程序

交付程序部分的测评方法如下：

a) 测评流程：

检查开发者提供的交付程序证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 现场检查开发者是否使用一定的交付程序交付产品；
2) 检查开发者是否使用文档描述交付过程,文档中是否包含以下内容:在给用户方交付系统的各版本时,为维护安全所必需的所有程序。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.3.3中所述的要求。

6.2.4 测试

6.2.4.1 测试覆盖

测试覆盖部分的测评方法如下：

a) 测评流程：

检查开发者提供的测试覆盖证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 检查开发者提供的测试覆盖文档,在测试覆盖证据中,是否表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.4.1中所述的要求。

6.2.4.2 功能测试

功能测试部分的测评方法如下：

a) 测评流程：

检查开发者提供的功能测试证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 现检查开发者提供的测试文档,是否包括测试计划、预期的测试结果和实际测试结果,检查 测试计划是否标识了要测试的安全功能,是否描述了每个安全功能的测试方案;

2) 检查期望的测试结果是否表明测试成功后的预期输出;

3) 检查实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。场检查开发者是否使用一定的交付程序交付产品。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.4.2中所述的要求。

6.2.4.3 独立测试

独立测试部分的测评方法如下：

a) 测评流程：

检查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致,以用于安全功能的抽样测试,并检查开发者提供的资源是否满足内容和形式的所有要求。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.4.3中所述的要求。

6.2.5 脆弱性评定

脆弱性评定部分的测评方法如下：

a) 测评流程：

从用户可能破坏安全策略的明显途径出发,按照安全机制定义的安全强度级别,对产品进行脆弱性分析;判断产品是否能抵抗中等型型攻击。

b) 预期结果：

渗透性测试结果应表明产品能抵抗中等型攻击。

6.2.6 代码安全

代码安全部分的测评方法如下：

a) 测评流程：

检查开发者提供的代码安全证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求，确认开发者采用了代码审计等方式，对 PKI 系统进行安全性测试并提供相关测试文档，确保

PKI 系统的代码安全。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 6.2.6中所述的要求。

7 增强级测评方法

7.1 安全功能测评方法

7.1.1 通用密钥管理

7.1.1.1 密钥有效期设置

密钥有效期设置部分的测评方法如下：

a) 测评流程：

1) 确认 PKI 系统的密钥管理模块（子系统）在生成密钥时，为密钥设置了有效期，密钥的有效期设置是否考虑了 GB/T 21053 7.1.1.1 中列出的因素；
2) 确认密钥的有效期设置是否符合国家密码行政管理部门相关规定。

b) 预期结果：

1) PKI 系统的密钥管理模块（子系统）在生成密钥，依据 GB/T 21053 7.1.1.1 中列出的因素为密钥设置了有效期；
2) 密钥的有效期设置符合国家密码行政管理部门相关规定。

7.1.1.2 密钥导入导出

密钥导入导出部分的测评方法如下：

c) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了密钥导入导出方法，包括：允许导入导出的密钥类型、执行密钥导入导出时应具有的权限、具体的密钥导入导出流程等等；
2) 结合文档和对实际系统的分析，确定密钥导入导出时是否采用国家密码行政管理部门认可的加密算法或加密设备。
3) 结合文档和对实际系统的分析，确定各类私钥的导入导出流程，确认导入导出过程中，密钥是否始终以加密形式存在；
4) 确认 PKI 系统是否具有将导入导出密钥与实体关联和赋予权限的机制，例如：在导入密钥时，要求输入密钥的所有者信息、在系统中维护密钥索引与用户实体的映射列表、针对导入导出密钥的权限分配列表等等；
5) 通过尝试访问登录实体无权限使用的密钥等方式，确定 PKI 系统是否实现了对导入导出密钥的管理。

d) 预期结果：

1) PKI 系统文档中明确规定了密钥导入导出方法；密钥的实际导入导出方法与文档中的规定一致；
2) PKI 系统的各类私钥不应以明文形式导入导出 PKI 系统，PKI 系统用户密钥和系统部件密钥应由国家密码行政管理部门认可的硬件密码设备加密，终端用户密钥可使用软件加密，CA 签名私钥应使用硬件密码设备加密。
3) 各类私钥的导入导出过程中，密钥始终以加密形式存在；
4) PKI 系统提供了将导入导出密钥与实体关联并赋予权限的机制；

5） 对于与导入导出密钥赋予权限不匹配的密钥操作，PKI 系统拒绝执行。

7.1.1.3 密钥归档

7.1.1.3.1 私钥归档

私钥归档部分的测评方法如下：

a) 测评流程：

1） 确定 PKI 系统文档中是否明确规定了私钥归档方法，包括：执行密钥归档的条件、密钥归档的对象、执行密钥归档操作的具体流程等；
2） 结合文档和对实际系统的分析，确定密钥归档操作是否与文档中的规定一致；
3） 分析密钥归档记录，确认其中是否包含签名私钥；
4） 分析密钥归档记录，确认其中是否包含所有应被归档的用于解密数据的私钥。

b) 预期结果：

1） PKI 系统文档中明确规定了私钥归档方法；在实际系统中，密钥归档方法与文档中规定的一致；归档方法确保签名私钥不能被归档。
2） 密钥归档记录中不包含任何的签名私钥；
3） 密钥归档记录中包含所有应被归档的用于解密数据的私钥。

7.1.1.3.2 公钥归档

公钥归档部分的测评方法如下：

a) 测评流程：

1） 确定 PKI 系统文档中是否明确规定了公钥归档方法，包括：执行密钥归档的条件、密钥归档的对象、执行密钥归档操作的具体流程等；
2） 结合文档和对实际系统的分析，确定密钥归档操作是否与文档中的规定一致；
3） 分析密钥归档记录，确认其中是否包含所有应被归档的 CA、RA、终端用户或其他系统部件的公钥。

b) 预期结果：

1） PKI 系统文档中明确规定了公钥归档方法；在实际系统中，密钥归档方法与文档中规定的一致；
2） 密钥归档记录中包含所有应被归档的 CA、RA、终端用户或其他系统部件的公钥。

7.1.2 PKI 系统密钥管理

7.1.2.1 PKI 系统密钥生成

PKI 系统密钥生成部分的测评方法如下：

c) 测评流程：

1） 确定 PKI 系统文档中是否明确规定了 PKI 系统密钥生成方法；包括：对于各种类型的密钥，有权限执行密钥生成操作的实体或系统、密钥生成服务的信息及相关资质、密钥生成操作的流程、密钥生成操作的具体算法、密钥生成涉及随机数的生成方式等等；
2） 结合文档，确定 PKI 系统的系统用户密钥是否由 CA 或 RA 等机构生成；
3） 尝试执行 PKI 系统的 CA 密钥生成过程，确定 CA 密钥生成操作是否仅能够在多个管理员同时在场的情况下执行；
4） 结合文档，确认 CA 签名公私钥对的生成方法使用硬件密码设备产生，经过国家行政管理部门认可。

d) 预期结果：

1） PKI 系统文档中明确规定了密钥生成方法；

2) PKI 系统的系统用户密钥由 CA 或 RA 等机构生成；

3) 当且仅当多个管理员同时在场并进行鉴别的情况下，才能执行 PKI 系统的 CA 密钥生成过程；

4) CA 签名公私钥对由硬件设备生成，生成方法经过国家行政管理部门认可，并满足 GB/T 21053 中所列出的要求。

7.1.2.2 PKI 系统密钥传送与分发

PKI 系统密钥传送与分发部分的测评方法如下：

a) 测评流程：

1) 结合文档等确定 PKI 系统中部件密钥、系统用户密钥、CA 密钥等各类系统密钥的传送与分发方法；

2) 结合文档和对实际传递消息的分析，确定部件密钥和系统用户密钥的传送与分发是否进行了加密；确定加密密钥的生成方式；

3) 结合文档和对实际传递消息的分析，确定 CA 公钥分发方法是否具有可行性，是否对 CA 公钥应用了数字签名或消息鉴别码等完整性保护机制；

4) 确定 PKI 系统文档中是否明确规定了 CA 密钥分发方法；包括：CA 密钥传送过程的参与方、具体的流程、使用的完整性保护机制和加密机制等。

b) 预期结果：

1) 能够确定 PKI 系统中部件密钥、系统用户密钥、CA 密钥和终端用户密钥等各类密钥的传送与分发方法；实际的传送和分发方法与文档中的规定一致；

2) 部件密钥和系统用户密钥的传送与分发进行了加密；加密密钥的生成采用了密钥协商等安全方法；

3) CA 公钥分发方法具有可行性，对 CA 公钥进行了完整性保护；

4) PKI 系统文档中明确规定了 CA 密钥分发方法。

7.1.2.3 PKI 系统密钥存储

PKI 系统密钥存储部分的测评方法如下：

a) 测评流程：

1） 确定 PKI 系统文档中是否明确规定了系统密钥存储方法；包括：部件密钥、系统用户密钥、CA 密钥等各类密钥的存储位置、密钥存储操作的执行流程、对以加密形式存储密钥进行解密的方法、对密钥存储介质和系统的管理机制等；

2) 结合文档和对实际存储介质的分析，确定 PKI 系统部件密钥和系统用户密钥的存储方式是否为以下方式之一：存储于密码模块中；以加密的形式存储；

3) 当使用密码模块时，确定密码模块是否符合国家密码行政管理部门规定；当使用加密形式存储时，确定对加密密钥的管理方式是否存在可能的安全风险，包括：在存储介质中以明文形式保存加密密钥、在代码中写入明文形式的加密密钥等等；

4) 结合文档和对实际存储介质的分析，确定 CA 签名公私钥是否存储于硬件密码设备中；使用的硬件密码设备是否经过国家密码行政管理部门认可。

b) 预期结果：

1) PKI 系统文档中明确规定了各类系统密钥的存储方法；密钥的实际存储方法与文档中的规定一致；

2) PKI 系统部件密钥和系统用户密钥存储于国家密码行政管理部门规定密码模块中；以加密的形

式存储；对加密密钥进行了安全管理；

3) CA 签名公私钥存储于硬件密码设备中；使用的硬件密码设备经过国家密码行政管理部门认可。

7.1.2.4 PKI 系统密钥备份

PKI 系统密钥备份部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了密钥备份方法，包括：密钥备份操作流程、采用的密钥备份方法等等；
2) 结合文档和对实际系统的分析，确定 PKI 系统部件密钥和系统用户密钥备份过程中，密钥是否始终以加密形式存在；
3) 结合文档和对实际系统的分析，确定 CA 签名私钥备份过程中，密钥是否始终以加密形式存在；
4) 尝试在未授权情况下访问 CA 私钥信息的存放部件，如：硬件密码设备等，确定存放部件是否存在访问控制机制；
5) 确定是否存在由 PKI 系统备份用户机密性目的密钥的情况，如果存在，结合文档和对实际系统的分析，确定在备份过程中，密钥是否始终以加密形式存在。

b) 预期结果：

1) PKI 系统文档中明确规定了密钥备份方法；密钥的实际备份方法与文档中的规定一致；
2) 在 PKI 系统部件密钥和系统用户密钥备份过程中，密钥是否始终以加密形式存在；
3) 在 CA 签名私钥备份过程中，密钥是否始终以加密形式存在；
4) CA 私钥信息的存放部件实施了有效的访问控制机制，未授权情况下，无法访问存放部件；
5) 如果存在由 PKI 系统备份用户机密性目的密钥的情况，则在密钥备份过程中，密钥是否始终以加密形式存在。

7.1.2.5 PKI 系统密钥更新

PKI 系统密钥更新部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了系统密钥更新方法，包括：执行密钥更新的条件、允许执行密钥更新的用户、密钥更新的具体流程等等；
2) 确定 PKI 系统是否提供了明确的 CA 密钥及证书更新方法,并对 CA 密钥更新时 PKI 系统服务的安全性和连续性进行了明确说明；结合文档和对实际系统的分析，确定上述措施是否在 PKI 系统中得到了实施；
3) 分析并确定 CA 密钥及证书更新中涉及密钥生成、分发、归档、销毁等操作，确定这些操作是否满足本级别中各自的相关规定。

b) 预期结果：

1) PKI 系统文档中明确规定了系统密钥更新方法；
1) PKI 系统提供了明确的 CA 密钥及证书更新方法,其中包含必要的措施来保障 CA 密钥更新时 PKI 系统服务的安全性和连续性，在实际系统中，CA 密钥及证书更新方法与文档中规定的一致；
2) CA 密钥及证书更新中涉及密钥生成、分发、归档、销毁等操作满足本级别中各自的相关规定。

7.1.2.6 PKI 系统密钥恢复

PKI 系统密钥恢复部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了系统密钥恢复方法，包括：执行密钥恢复的条件、允许执

行密钥恢复操作的用户应具有的权限、执行密钥恢复操作时的具体流程、涉及法律、规章、执法机关或管理部门等等；

2) 尝试执行备份密钥恢复操作，确认 PKI 系统应在恢复密钥前验证申请者的身份，确认是否只有密钥所有者能够成功执行密钥恢复操作；

3) 尝试执行归档密钥恢复操作，确认 PKI 系统是否依据文档中规定的归档密钥恢复流程，按照法律、规章或合同生成恢复请求；

4) 结合文档和对实际系统的分析，确定密钥恢复过程中是否实现了访问控制和完整性保护机制，以防止密钥不被未授权地泄露或修改,例如:使用密钥持有者的密钥进行加密以防止密钥泄露；使用系统部件私钥对密钥进行签名，防止密钥被修改等；

5) 结合文档和对实际系统的分析，确定 CA 签名私钥恢复过程是否实施了人员权限确认和环境可信保护机制。

b) 预期结果：

1) PKI 系统文档中明确规定了系统密钥恢复方法；在实际系统中，密钥恢复方法与文档中规定的一致；

2) PKI 系统在执行备份密钥恢复操作前，验证申请者的身份，只有密钥所有者能够成功执行密钥恢复操作；

3) PKI 系统按照归档密钥恢复操作的流程执行操作，生成恢复请求，供执行密钥恢复操作的执法机关或管理部门使用。相关流程与法律、规章或合同一致。

4) 在 CA 签名私钥恢复过程中，实施了人员权限确认和环境可信保护机制。

7.1.2.7 PKI 系统密钥销毁

PKI 系统密钥销毁部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了系统密钥销毁方法，包括：执行密钥销毁人员应具有的权限、密钥销毁流程等等；

2) 确认密钥销毁方法是否包含了对执行人权限的确认,尝试使用不具有权限的人员执行密钥销毁操作，确认密钥销毁操作能否被执行；

3) 确认PKI 系统文档中是否提供了PKI 系统密钥销毁流程与国家密码行政管理部门对密钥销毁的相关规定的符合性说明；

4) 结合文档和对实际系统的分析，确定密钥销毁操作是否与文档中的规定一致。

b) 预期结果：

1) PKI 系统文档中明确规定了系统密钥销毁方法；在实际系统中，密钥销毁方法与文档中规定的一致；

2) 密钥销毁方法中包含对执行人权限的确认，不具有权限的人员不能执行密钥销毁程序；

3) 结合文档和对实际系统的分析,可以确定 PKI 系统密钥销毁符合国家密码行政管理部门对密钥销毁的相关规定。

7.1.3 用户密钥管理

7.1.3.1 终端用户密钥生成

终端用户密钥生成部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了用户密钥生成方法；

2） 结合文档，确认终端用户的密钥生成方法，确定终端用户的密钥是否是由用户自己生成或委托CA、RA 等 PKI 系统的服务机构生成；

3） 确认 PKI 系统是否提供终端用户密钥生成机制,提供的密钥生成机制采用国家密码行政管理部门认可的硬件设备。

b) 预期结果：

1） PKI 系统文档中明确规定了密钥生成方法；

2） 终端用户的密钥生成方法与文档一致，终端用户签名私钥由其自己生成；终端用户加密密钥由用户自己生成，或委托 CA、RA 等 PKI 系统的服务机构生成。

3） 终端用户自己生成密钥时，PKI 系统提供了终端用户密钥生成机制，采用国家密码行政管理部门认可的硬件设备生成。

7.1.3.2 终端用户密钥传送与分发

终端用户密钥传送与分发部分的测评方法如下：

a) 测评流程：

1） 结合文档等确定终端用户密钥等各类密钥的传送与分发方法；

2） 确定终端用户的密钥生成方式；如果终端用户自己生成密钥对，确定终端用户向 PKI 系统提交用户公钥的流程中，是否对用户公钥应用了数字签名或消息鉴别码等完整性保护机制；如果终端用户委托 CA 生成密钥对，确定 CA 向用户传送与分发私钥时，是否对用户私钥进行了加密，确定加密密钥的生成方式；。上述过程应结合文档和对实际传递消息的分析进行；

3） 确定 PKI 系统文档中是否明确规定了用户公钥传送方法；包括：用户公钥传送过程的参与方、具体的流程、使用的完整性保护机制等。

b) 预期结果：

1） 能够确定 PKI 系统中终端用户密钥等各类密钥的传送与分发方法；实际的传送和分发方法与文档中的规定一致；

2） 终端用户自己生成密钥对时，终端用户向 PKI 系统提交用户公钥的流程中，对用户公钥进行了完整性保护；

3） 终端用户委托 CA 生成密钥对时，CA 向用户传送与分发私钥时，对用户私钥进行了加密；加密密钥的生成采用了密钥协商等安全方法；

4） PKI 系统文档中明确规定了用户公钥传送方法。

7.1.3.3 终端用户密钥存储

终端用户密钥存储部分的测评方法如下：

a) 测评流程：

1） 确定 PKI 系统文档中是否明确规定了终端用户密钥存储方法；包括：密钥的存储位置、密钥存储操作的执行流程、对以加密形式存储密钥进行解密的方法、对密钥存储介质和系统的管理机制等；

2） 结合文档确定终端用户密钥的存储方式，如果终端用户的密钥在 PKI 系统服务部件中存储，确定在存储时是否进行了加密；确定对加密密钥的管理方式是否存在可能的安全风险，包括：在存储介质中以明文形式保存加密密钥、在代码中写入明文形式的加密密钥等等。

b） 预期结果：

1） PKI 系统文档中明确规定了各类密钥的存储方法；密钥的实际存储方法与文档中的规定一致；

2） 如果终端用户的密钥在 PKI 系统服务部件中存储，则密钥以加密的形式存储；对加密密钥进行了安全管理；

7.1.3.4 终端用户密钥备份

终端用户密钥备份部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了终端用户密钥备份方法，包括：密钥备份操作流程、采用的密钥备份方法等等；
2) 确定是否存在由 PKI 系统备份用户机密性目的密钥的情况，如果存在，结合文档和对实际系统的分析，确定在备份过程中，密钥是否始终以加密形式存在，加密算法是否符合国家密码行政管理部门的规定。

b) 预期结果：

1) CA 私钥信息的存放部件实施了有效的访问控制机制，未授权情况下，无法访问存放部件；
2) 如果存在由 PKI 系统备份用户机密性目的密钥的情况，则在密钥备份过程中，密钥是否始终以加密形式存在，加密算法符合国家密码行政管理部门的规定。

7.1.3.5 终端用户密钥更新

密钥更新部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了终端用户密钥更新方法，包括：执行密钥更新的条件、允许执行密钥更新的用户、密钥更新的具体流程等等；
2) 确定用户密钥是否由 PKI 系统自动更新，如果是，确定 PKI 系统是否提供了明确的用户密钥和证书更新方法，并对用户密钥更新时的安全性保障措施进行了说明；结合文档和对实际系统的分析，确定上述措施是否在 PKI 系统中得到了实施；
3) 分析并确定用户密钥及证书更新中涉及密钥生成、分发、归档、销毁等操作，确定这些操作是否满足本级别中各自的相关规定。

b) 预期结果：

1) PKI 系统文档中明确规定了终端用户密钥更新方法；
2) 如果终端用户密钥由 PKI 系统自动更新，则 PKI 系统提供了明确的用户密钥及证书更新方法，其中包含必要的措施来保障用户密钥更新时的安全性，在实际系统中，用户密钥及证书更新方法与文档中规定的一致；
3) 终端用户密钥及证书更新中涉及密钥生成、分发、归档、销毁等操作满足本级别中各自的相关规定。

7.1.3.6 终端用户密钥恢复

终端用密钥恢复部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统文档中是否明确规定了终端用户密钥恢复方法，包括：执行密钥恢复的条件、允许执行密钥恢复操作的用户应具有的权限、执行密钥恢复操作时的具体流程、涉及法律、规章、执法机关或管理部门等等；
2) 尝试执行备份密钥恢复操作，确认 PKI 系统应在恢复密钥前验证申请者的身份，确认是否只有密钥所有者能够成功执行密钥恢复操作；
3) 尝试执行归档密钥恢复操作，确认 PKI 系统是否依据文档中规定的归档密钥恢复流程，按照法律、规章或合同生成恢复请求；
4) 结合文档和对实际系统的分析，确定密钥恢复过程中是否实现了访问控制和完整性保护机制，

以防止密钥不被未授权地泄露或修改,例如:使用密钥持有者的密钥进行加密以防止密钥泄露;使用系统部件私钥对密钥进行签名，防止密钥被修改等。

b) 预期结果：

1） PKI 系统文档中明确规定了密钥恢复方法;在实际系统中,密钥恢复方法与文档中规定的一致;

2） PKI 系统在执行备份密钥恢复操作前，验证申请者的身份，只有密钥所有者能够成功执行密钥恢复操作;

3） PKI 系统按照归档密钥恢复操作的流程执行操作，生成恢复请求，供执行密钥恢复操作的执法机关或管理部门使用。相关流程与法律、规章或合同一致。

7.1.3.7 终端用户密钥销毁

终端用户密钥销毁部分的测评方法如下：

a) 测评流程：

1） 确定 PKI 系统文档中是否明确规定了终端用户密钥销毁方法，包括：密钥销毁流程等等。

b) 预期结果：

1） PKI 系统文档中明确规定了终端用户密钥销毁方法。

7.1.4 轮廓管理

7.1.4.1 证书轮廓管理

证书轮廓管理部分的测评方法如下：

a) 测评流程：

1) 根据文档，确定 PKI 系统是否具有证书轮廓;

2) 验证证书轮廓中的信息,确定证书轮廓中所定义的字段和扩展是否均为 GB/T 20518-2018 中所规定的字段和扩展;

3) 确定证书轮廓中是否包含以下所有信息:

——与密钥绑定的用户的标识符;

——主体的公私密钥对可使用的加密算法;

——证书发布者的标识符;

——证书有效时间的限定;

——证书包括的附加信息;

——证书的主体是否是 CA;

——与证书相对应的私钥可执行的操作;

——证书发布所使用的策略。

4) 确定证书轮廓中，是否为所有以下字段和扩展指定了可能的取值:

——密钥所有者的标识符;

——公私密钥对主体的算法标识符;

——证书发布者的标识符;

——证书的有效期。

——keyUsage;

——basicConstraints;

——certificatePolicies;

5) 对比 PKI 系统颁发的证书，确定所有证书的内容是否与证书轮廓一致;

b) 预期结果：

1) PKI 系统具有证书轮廓；
2) 证书轮廓中所定义的字段和扩展均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 证书轮廓中包含所列出的各项信息；
4) 证书轮廓中为列出的所有字段和扩展指定了可能的取值；
5) 进行验证的所有证书的内容与证书轮廓一致。

7.1.4.2 证书撤销列表轮廓管理

证书撤销列表轮廓管理部分的测评方法如下：

a) 测评流程：

1) 根据文档，确定 PKI 系统是否发布 CRL，如果发布 CRL，PKI 系统是否具有证书撤销列表轮廓；
2) 验证证书撤销列表轮廓中的信息，确定证书撤销列表轮廓中所定义的字段和扩展是否均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 确定证书轮廓中，是否为所有以下字段和扩展指定了可能的取值：

——issuer;

——issuerAltName；

——NextUpdate。

4) 确认管理员是否能够指定 CRL 和 CRL 扩展可接受的值。
5) 对比 PKI 系统颁发的 CRL，确定所有 CRL 的内容是否与证书撤销列表轮廓一致。

b) 预期结果：

1) 如果 PKI 系统发布 CRL，PKI 系统具有证书撤销列表轮廓；
2) 证书撤销列表轮廓中所定义的字段和扩展均为 GB/T 20518-2018 中所规定的字段和扩展；
3) 证书撤销列表轮廓中包含所列出的各项信息；
4) **管理员能够为证书撤销列表轮廓中为列出的所有字段和扩展指定了可能的取值**；
5) 进行验证的所有 CRL 的内容与证书撤销列表轮廓一致。

7.1.4.3 在线证书状态协议轮廓管理

OCSP 轮廓管理部分的测评方法如下：

a) 测评流程：

1) 根据文档，确定 PKI 系统是否发布 OCSP 响应，如果发布 OCSP 响应，PKI 系统是否具有在线证书状态协议轮廓；
2) 确定在线证书状态协议轮廓中，是否为 responseType 字段指定了可接受的值；
3) 若 PKI 系统允许使用基本相应类型（basic response type）的 OCSP 响应，确定在线证书状态协议轮廓中，是否为 ResponseID 字段指定了可接受的值；
4) 结合文档，构建测试用 OCSP 请求，将 OCSP 请求发送至 PKI 系统的 OCSP 服务并记录返回的消息，确认该消息与在线证书状态协议轮廓中的描述一致。

b) 预期结果：

1) 如果 PKI 系统发布 OCSP 响应，PKI 系统具有在线证书状态协议轮廓；
2) 在线证书撤销列表轮廓中为 responseType 指定了可能的取值；
3) 若 PKI 系统允许使用基本相应类型，在线证书状态协议轮廓中为 ResponseID 字段指定了可接受的值；
4) 进行验证获取的所有 OCSP 响应的内容与在线证书状态协议轮廓一致。

7.1.5 证书管理

7.1.5.1 证书注册

证书注册部分的测评方法如下：

a) 测评流程：

1) 生成测试证书请求，提交至 PKI 系统执行证书注册流程，确定 PKI 系统是否对输入证书字段和扩展中的数据进行了批准，确定 PKI 系统对证书数据的批准方式；
2) 检查通过测试证书注册流程获取的证书，确定其格式是否符合 GB/T 20518-2018 的要求；
3) 结合 PKI 系统的证书轮廓检查通过测试证书注册流程获取的证书，确定颁发的证书是否与证书轮廓中定义相符；
4) 若 PKI 系统允许用户密钥对由用户生成，则执行证书请求，选择由用户生成密钥对，然后使用不知道对应私钥作为证书请求的公钥，确定 PKI 系统是否对证书主体拥有与证书中包含的公钥相对应的私钥；
5) 检查通过测试证书注册流程获取的证书，确定其内容是否符合以下要求：

——version 字段应为 0,1,2；
——若包含 issuerUniqueID 或 subjectUniqueID 字段，则 version 字段应为 1 或 2；
——若证书包含 extensions，那么 version 字段应为 2；
——serialNumber 字段对 CA 应是唯一的；
——validity 字段应说明不早于当时时间的 notBefore 值和不早于 notBefore 时间的 notAfter 值；
——若 issuer 字段为空，证书应包括一个 issuerAltName 的关键性扩展；
——若 subject 字段为空，证书应包括一个 subjectAltName 的关键性扩展；
——subjectPublicKeyInfo 字段中的 signature 字段和 algorithm 字段应包含国家密码行政管理部门许可的或推荐的算法的 OID。

b) 预期结果：

1) PKI 系统的证书注册流程中包含对输入证书字段和扩展中的数据进行批准的操作，批准方式为以下方式之一：

——数据被操作员手工批准；
——自动过程检查和批准数据；
——字段或扩展的值由 PKI 系统自动生成；
——字段或扩展的值从证书轮廓中获得。

2) 当方式为手工批准或自动检查和批准时，不符合要求的数据不会被批准；
3) 若 PKI 系统允许用户密钥对由用户生成，则 PKI 系统对证书主体拥有与证书中包含的公钥相对应的私钥，不持有与公钥对应的私钥情况下，证书注册请求无法完成；
4) 通过测试证书注册流程获取的证书，其内容符合本节中的要求。

7.1.5.2 证书撤销

7.1.5.2.1 证书撤销列表审核

证书撤销列表审核部分的测评方法如下：

a) 测评流程：

确定 PKI 系统是否发布 CRL，如果发布，则执行以下流程：

1) 结合文档与对实际系统的分析，确定 PKI 系统是否实现了证书撤销列表审核机制；
2) 确认证书撤销列表审核机制是否验证 CRL 的所有强制性字段的值符合 GB/T 20518-2018。并实

现了对以下内容的检查：

——若包含 version 字段，应为 1；

——若 CRL 包含关键性的扩展，version 字段应出现且为 1；

——signature 和 signatureAlgorithm 字段应为许可的数字签名算法的 OID；

——thisUpdate 应包含本次 CRL 的发布时间；

——nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

3) 查看 PKI 系统发布的 CRL，确认发布的 CRL 的内容是否与规定的证书撤销列表审核机制一致。

b) 预期结果：

如果 PKI 系统发布 CRL，则按照以下预期结果进行确认：

1) PKI 系统实现了证书撤销列表审核机制；

2) 证书撤销列表审核机制验证 CRL 的所有强制性字段的值符合 GB/T 20518-2018。并实现了对相关内容的检查；

3) 发布的 CRL 的内容与规定的证书撤销列表审核机制一致。

7.1.5.2.2 OCSP 基本响应的审核

OCSP 基本响应审核部分的测评方法如下：

a) 测评流程：

确定 PKI 系统是否发布 OCSP 响应，如果发布，则执行以下流程：

1) 结合文档与对实际系统的分析，确定 PKI 系统是否实现了 OCSP 基本响应审核机制；

2) 确认 OCSP 基本响应审核机制是否验证所有强制性字段的值符合 GB/T 17913-2005；

3) 确认 OCSP 基本响应审核机制是否实现了对以下内容的检查：

——Version 字段应为 0；

——signatureAlgorithm 字段应为许可的数字签名算法的 OID；

——thisUpdate 字段应指出证书状态正确的时间；

——producedAt 字段应指出 OCSP 响应者发出响应的时间；

——nextUpdate 字段的时间不应早于 thisUpdate 字段的时间。

4) 查看 PKI 系统发布的 OCSP 响应，确认发布的 OCSP 响应的内容是否与规定的 OCSP 基本响应审核机制一致。

b) 预期结果：

如果 PKI 系统发布 OCSP 响应，则按照以下预期结果进行确认：

1) PKI 系统实现了 OCSP 基本响应审核机制审核机制；

2) OCSP 基本响应审核机制验证所有强制性字段的值符合 GB/T 17913-2005；

3) OCSP 基本响应审核机制实现了对相关内容的检查；

4) 发布的 OCSP 响应的内容与规定的 OCSP 基本响应审核机制一致。

7.1.6 身份鉴别

7.1.6.1 用户属性定义

用户属性定义部分的测评方法如下：

a) 测评流程：

确定 PKI 系统是否维护用户属性定义，即对于每个用户，给出该用户所具有的属性信息，维护属性定义的方式包括：将属性定义记录在用户数据库中、为用户颁发属性证书等等。

b) 预期结果：

PKI系统提供了相应机制维护用户属性定义。

7.1.6.2 用户身份鉴别

用户鉴别部分的测评方法如下：

a) 测评流程：

1) 确定 PKI 系统提供了相应机制，是否定义了在标识用户前可以由 PKI 系统代表用户执行的、与安全功能无关的动作，例如：响应查询公开信息；接收用户发来的数据，但直到系统用户批准之后才处理等等。确认这些事件的设置是否适当；
2) 在不进行鉴别的情况下，执行与安全无关的操作，确定操作能否被执行；
3) 在不进行鉴别的情况下，执行其它的安全功能引起的操作动作，确定操作能否被执行，是否要求用户进行鉴别；
4) 在进行鉴别的情况下，使用当前用户能够执行的安全功能引起的操作动作，确定操作能否被执行；
5) **查看 PKI 文档，确定 PKI 系统是否提供了多种不同鉴别机制，结合用户属性分配，确定若干应使用不同鉴别机制的用户，使用这些用户分别进行鉴别，确定 PKI 系统是否执行了不同的鉴别机制，鉴别机制包括：使用用户名/口令、使用用户证书、使用生物特征识别等等；**
6) 在用户鉴别时，观察 PKI 系统的反馈，确定是否存在违反最小信息原则的或泄露用户的鉴别数据，例如：输入的口令被显示。

b) 预期结果：

1) PKI 系统设置了适当的在标识用户前可以由 PKI 系统代表用户执行的，这些操作与安全无关；
2) 在不进行鉴别的情况下，预先设置的、与安全无关的操作能够被执行；
3) 在不进行鉴别的情况下，执行其它的安全功能引起的操作动作时，PKI 系统要求用户进行鉴别，如果不进行鉴别，则操作不能够被执行；
4) 在进行鉴别的情况下，符合策略的安全功能引起的操作动作能够被执行；
5) **PKI 系统提供了多种不同鉴别机制，当使用不同身份的用户进行鉴别时，能够触发不同的鉴别机制，当对一个用户同时使用多个鉴别过程进行鉴别时，所使用的鉴别机制中应包含基于数字证书的鉴别机制；**
6) 用户鉴别时 PKI 系统的反馈信息遵循最小信息原则，不包含用户鉴别信息。

7.1.6.3 鉴别失败处理

鉴别失败处理部分的测评方法如下：

a) 测评流程：

1) 执行 PKI 系统的鉴别操作，采用输入不正确的口令、提供不合法的用户证书等方式，执行失败的鉴别操作。确定 PKI 系统的安全功能是否能够检测到鉴别尝试不成功。
2) 结合 PKI 文档与相关配置信息，确定 PKI 系统是否设置了鉴别失败次数界限，然后对同一个用户，重复执行 1）中的操作，直至尝试次数达到定义的界限，确定 PKI 系统是否能够检测到此事件的发生；
3) **确认 PKI 系统实现了鉴别失败处理功能，当用户自最近一次鉴别成功以来不成功的鉴别尝试的次数达到或超过了定义的界限时，PKI 系统是否采取应对措施；**
4) **从拒绝服务攻击角度进行测试，确认 PKI 系统实施鉴别失败处理时，是否能够保证至少有一个用户账号不应失效。**

b) 预期结果：

1) 当进行不成功的鉴别尝试时，PKI 系统能够检测到该次鉴别不成功；
2) PKI 系统设置了鉴别失败次数界限；
3) 当达到预先设置的失败次数界限时，PKI 系统能够检测到此事件的发生。
4) **PKI 系统实现了鉴别失败处理功能，当用户自最近一次鉴别成功以来不成功的鉴别尝试的次数**

达到或超过了定义的界限时，PKI 系统能够采取应对措施；

5） PKI 系统实施鉴别失败处理时，能够保证至少有一个用户账号不应失效，能够防止拒绝服务攻击。

7.1.6.4 秘密的规范

秘密的规范部分的测评方法如下：

a) 测评流程：

1） 确认用来进行用户身份鉴别的秘密信息（如口令、密钥等）的产生方式；

2） 确认 PKI 系统是否提供了秘密信息质量的设置功能，设置秘密信息质量策略，确认秘密信息质量要求是否覆盖了 GB/T 21053 7.1.6.4 的要求；

3） 如果用户身份鉴别的秘密信息由终端用户自己产生时，然后生成符合与不符合要求的秘密，并尝试作为用户的秘密信息，确认 PKI 系统是否对秘密信息质量进行了检查；

4） 如果用户身份鉴别的秘密信息由 PKI 系统产生，则执行秘密生成操作，并检查生成的秘密信息质量是否符合设置的秘密信息质量。

b) 预期结果：

1） PKI 系统提供了秘密信息质量的设置功能，秘密信息质量要求覆盖了 GB/T 21053 7.1.6.4 的要求；

2） 当用户身份鉴别的秘密信息由终端用户自己产生时，PKI 系统能够依据设置的秘密信息质量规范进行检查，对于不符合规范的秘密信息，PKI 系统拒绝接受；

3） 当用户身份鉴别的秘密信息由 PKI 系统产生时，PKI 系统产生的秘密信息质量符合设置的秘密信息质量规范。

7.1.7 访问控制

7.1.7.1 角色与责任

角色与责任部分的测评方法如下：

a) 测评流程：

1) 配置 PKI 系统；

2) 查看 PKI 系统使用文档，确定是否存在对系统管理员、操作员和**审计员**的角色定义；

3) 结合 PKI 文档对系统中的权限分配相关信息，包括：权限分配表、访问控制数据库、属性证书等进行分析，确定 PKI 系统中角色和权限的对应关系是否符合 GB/T 21053-XXXX 表 5；

4) 根据 GB/T 21053-XXXX 表#中所列出的操作，规划测试流程，测试流程应涵盖表#中所列出的所有操作，包括：安装、配置、维护系统；建立和管理用户账户；配置轮廓和审计参数；生成部件密钥；查看和维护审计日志；执行系统的备份和恢复；签发和撤销证书；

5) 使用具有系统管理员角色的主体登录系统，执行测试流程中所列出的所有操作；

6) 使用具有操作员角色的主体登录系统，执行测试流程中所列出的所有操作；

7) **使用具有审计员角色的主体登录系统，执行测试流程中所列出的所有操作；**

8) 验证 PKI 系统是否具有将主体与角色进行关联的能力；

9) 执行角色分配操作，尝试为测试主体分配系统管理员、操作员和审计员中的两个或更多数量的角色。

b) 预期结果：

1) PKI 系统开发者提供了对系统管理员、操作员和审计员的角色定义；

2) PKI 系统中角色和权限的对应关系符合 GB/T 21053-XXXX 表 5；

3) 当使用具有系统管理员角色的主体登录系统时，能够执行与系统管理员角色对应的所有操作，

包括：安装、配置、维护系统；建立和管理用户账户；配置轮廓和审计参数；生成部件密钥；执行系统的备份和恢复。但对于其它操作，PKI 系统提示不具有相应权限；

4) 当使用具有操作员角色的主体登录系统时，能够执行与操作员角色对应的所有操作，包括：签发和撤销证书。但对于其它操作，PKI 系统提示不具有相应权限；

5) 当使用具有操作员角色的主体登录系统时，能够执行与操作员角色对应的所有操作，包括：查看和维护审计日志；但对于其它操作，PKI 系统提示不具有相应权限；

6) PKI 系统中应具有将主体与角色进行关联的能力；

7) 无法执行为测试主体分配系统管理员、操作员和审计员中的两个或更多数量角色的操作。

7.1.7.2 网络访问控制

网络访问控制部分的测评方法如下：

a) 测评流程：

1) 尝试通过网络对 PKI 系统服务进行访问，确定 PKI 系统对可能的路径提供了控制；

2) 使用远程计算机系统对 PKI 系统进行连接，确定是否需要进行认证；

3) 确定 PKI 系统是否提供了网络访问控制策略的定义；

4) 尝试访问 PKI 系统的诊断分析接口，确定是否需要进行认证，确定 PKI 系统是否对访问请求进行了记录；

5) 查看 PKI 文档，确定是否其中对所有网络服务的安全属性要求进行了说明；

6) 根据 PKI 系统中对于网络服务的安全属性要求的说明，设置测试操作的列表，对于每个网络服务，测试操作对于该网络服务的符合访问控制策略的服务请求和违背访问控制策略的服务请求；

7) 依据测试操作列表，执行每个测试操作，确定访问是否被限制和过滤。

b) 预期结果：

1) PKI 系统对系统服务的访问请求进行了控制，无法直接访问这些系统服务；

2) PKI 系统对远程计算机的所有连接请求进行认证，认证不通过时，无法连接到 PKI 系统；

3) PKI 系统提供了网络访问控制策略的定义；

4) PKI 系统对诊断分析接口的所有访问请求进行认证，认证不通过时，无法访问诊断分析接口；

5) PKI 系统对诊断分析接口的所有访问请求进行记录，记录包括访问时间、请求方的 IP 地址，认证结果；

6) PKI 文档中包含对于所有网络服务的安全属性要求进行了说明；

7) 测试操作列表中，所有符合访问控制策略的服务请求应能够正常执行；

8) 测试操作列表中，所有违背访问控制策略的服务请求应无法执行。

7.1.8 安全审计

7.1.8.1 审计数据产生

审计数据产生部分的测评方法如下：

a) 测评流程：

1) 结合 PKI 文档与相关配置信息，确定 PKI 系统是否提供了可审计事件维护功能；

2) 确定系统中已维护的所有可审计事件，确定 PKI 系统是否为每个审计事件生成了审计记录，审计记录中是否包含与审计事件相关的基本信息；

3) 选择性地与可审计事件相关的操作，然后查看审计记录，确定审计记录中记录了新发生的审计事件信息。

b) 预期结果：

1) PKI 系统提供了可审计事件维护功能，可以通过此功能对可审计事件进行维护；

2） PKI 系统为每个审计事件生成了审计记录，审计记录中包含与审计事件相关的基本信息；

3） 当执行与可审计事件相关的操作后，审计记录中能够增加新发生的审计事件信息。

7.1.8.2 审计查阅

审计查阅部分的测评方法如下：

a） 测评流程：

1） 结合 PKI 文档，确定 PKI 系统是否提供了审计记录查阅功能；

2） 确定审计查阅功能是否包含从审计记录中读取一定类型的审计信息的能力；

3） 选取若干审计信息类型，执行审计查阅，确定返回的审计记录与所选取的类型一致；

b） 预期结果：

1） PKI 系统是否提供了审计记录查阅功能；

2） 审计查阅功能包含从审计记录中读取一定类型的审计信息的能力；

3） 通过审计查阅功能，可以从审计记录中读取所选择类型的审计信息，返回的审计记录与所选取的类型一致。

7.1.8.3 选择性审计查阅

选择性审计部分的测评方法如下：

a） 测评流程：

1） 访问审计功能部件，结合 PKI 文档，确定审计功能部件是否提供了根据基本属性选择或排除审计事件集中的可审计事件的功能；

2） 执行可审计事件选择操作，选择和排除若干类型的可审计事件；

3） 选择性地与 2）中选择和排除的可审计事件相关的操作，然后查看审计记录，确定审计记录中是否记录了新发生的审计事件信息。

b） 预期结果：

1） 审计功能部件提供了根据基本属性选择或排除审计事件集中的可审计事件的功能；

2） 能够通过执行可审计事件选择操作，选择和排除特定类型的可审计事件；

3） 当选择某个类型的可审计事件后，执行与可审计事件相关的操作时，审计记录中能够增加新发生的审计事件信息；

4） 当排除某个类型的可审计事件后，执行与可审计事件相关的操作时，审计记录中不增加新发生的审计事件信息。

7.1.8.4 审计事件存储

审计事件存储部分的测评方法如下：

a） 测评流程：

1） 尝试以未授权形式对审计记录进行修改，例如：在不使用审计管理员进行鉴别的情况下，执行审计记录修改和删除操作；直接访问存储审计记录的数据库或文件，并进行修改；确定操作能否完成；

2） 尝试以授权形式对审计记录进行修改，例如：在使用审计管理员进行鉴别的情况下，执行审计记录修改操作；确定操作能否完成；

3） 确定审计功能部件是否提供了审计记录修改检测操作，在执行审计记录修改操作后，执行审计记录修改检测操作，确定审计功能部件能否检测到对审计记录的修改；

4） 将审计踪迹存储配置为已满状态，然后执行不由**审计员**发起的若干审计事件，确定审计功能部件是否阻止该事件的发生。

b） 预期结果：

1） 尝试以未授权形式对审计记录进行修改时，审计功能部件能够防止这些操作的执行，例如：执行操作时，提示权限不足；无法直接访问存储审计记录的数据库或文件等；

2） 尝试以授权形式对审计记录进行修改时，操作能够执行；
3） 审计功能部件提供了审计记录修改检测操作，执行审计记录修改检测操作，能够检测到对审计记录的修改，返回的修改记录与执行的修改操作一致；
4） 审计踪迹存储配置为已满状态时，审计功能部件应能够阻止由**审计员**发起的以外的所有审计事件的发生。

7.1.8.5 审计日志完整性保护

审计日志完整性部分的测评方法如下：

a) 测评流程：
1） 结合文档，确定审计功能部件是否提供了定期的审计日志完整性保护功能，确定是否使用基于数字签名等完整性保护机制对审计日志进行完整性保护；
2） 执行审计日志签名配置操作，确定是否能够对审计日志完整性保护运算的时间周期进行配置；
3） 查看审计日志，确定其中是否包含审计日志完整性保护运算的事件；确定审计日志完整性保护运算的周期是否与配置的周期一致；
4） 确定审计日志完整性保护运算的事件记录的信息中，是否包含用于完整性保护运算的审计日志范围和对审计日志签名的结果；
5） 根据文档中记录的审计日志完整性保护运算机制，确定 4）中的审计日志完整性保护运算的有效性。

b) 预期结果：
1） 审计功能部件提供了定期的审计日志完整性保护功能，使用了基于数字签名等的完整性保护机制；
2） 能够通过审计日志签名配置操作对审计日志完整性保护运算的时间周期进行配置；
3） 审计日志中包含系统运行期间所有的审计日志签名完整性保护运算事件；审计日志完整性保护运算事件的执行周期与配置的周期一致；当配置的时间周期发生改变时，审计日志签名完整性保护运算的执行周期与新配置的周期一致；
4） 审计日志完整性保护运算事件记录中，包含被签名的审计日志范围和对审计日志完整性保护运算的结果；
5） 4)中的审计日志完整性保护运算的结果应是对所配置的审计日志范围中的审计日志使用预先确定的完整性保护运算机制以及密钥等安全参数生成的。

7.1.9 原发抗抵赖

原发抗抵赖部分的测评方法如下：

a) 测评流程：
1） 结合 PKI 文档，确定 PKI 系统是否提供了原发抗抵赖权标生成功能，确定原发抗抵赖权标生成机制以及覆盖范围；
2） 结合文档，确定 PKI 系统是否实现了与文档一致的原发抗抵赖权标生成功能，原发抗抵赖机制是否覆盖了证书状态信息以及其他安全信息。
3） 结合 PKI 文档，确定原发抗抵赖权标中包含的信息，是否与原发信息者正确关联。

b) 预期结果：
1） PKI 系统是否提供了原发抗抵赖权标生成功能；
2） 原发抗抵赖权标生成功能能够正常执行，执行过程与文档一致；
3） 原发抗抵赖机制是否覆盖了证书状态信息以及其他安全信息，原发抗抵赖权标中包含的信息与原发信息者正确关联并能够依据正规的流程进行验证。

7.1.10 备份和恢复

备份与恢复部分的测评方法如下：

a) 测评流程：

1) 结合 PKI 文档，确定 PKI 系统是否提供了备份和恢复功能；
2) 尝试调用备份功能，确定在需要时是否能够调用备份功能生成系统备份数据；
3) 执行备份操作，然后对系统进行修改，然后尝试执行恢复功能，结合对备份数据的内容进行分析，确定是否能够通过系统备份数据重建备份时的系统状态；
4) **结合文档，确定 PKI 系统是否为备份数据提供了完整性保护措施，例如：对备份数据所存储的介质进行访问控制；对备份数据进行签名并定期或在执行恢复时进行校验；**
5) **结合 PKI 文档，确定备份数据中包含的关键安全参数和机密信息，例如：PKI 系统用户的口令等；**
6) **访问 5）中所确定的所有关键安全参数和机密信息，确定这些信息是否以加密形式存储。**

b) 预期结果：

1) PKI 系统提供了备份和恢复功能；
2) 备份功能能够正常执行，执行备份操作后，能够生成当前时间节点的系统备份数据；
3) 系统备份数据中保存了足够的信息，能够通过执行恢复功能重建备份时的系统状态；
4) **PKI 系统为备份数据提供了完整性保护措施；对于备份数据中包含的所有关键安全参数和机密信息，在备份数据中均以加密形式存储。**

7.2 安全保障测评方法

7.2.1 开发

7.2.1.1 安全架构

安全架构部分的测评方法如下：

a) 测评流程：

1) 检查开发者提供的安全架构证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:
2) 检查 PKI 系统与产品设计文档中对安全功能的描述范围是否相一致。

b) 预期结果：

开发者提供的信息应满足 GB/T 21053 7.2.1.1 中所述的要求。

7.2.1.2 功能规范

功能规范部分的测评方法如下：

a) 测评流程：

检查开发者提供的功能规范证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否清晰描述定义的产品安全功能;
2) 是否描述产品所有安全功能接口的目的、使用方法及相关参数;
3) 描述安全功能实施过程中,是否描述与安全功能接口相关的所有行为;
4) 是否描述可能由安全功能接口的调用而引起的所有直接错误消息。

b) 预期结果：

开发者提供的信息应满足 GB/T 21053 7.2.1.2 中所述的要求。

7.2.1.3 产品设计

产品设计部分的测评方法如下：

a) 测评流程：

检查开发者提供的产品设计证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否根据子系统描述产品结构,是否标识和描述产品安全功能的所有子系统,是否描述安全功能所有子系统间的相互作用；
2) 提供的对应关系是否能证实设计中描述的所有行为映射到调用的安全功能接口;
3) 是否根据实现模块描述安全功能,是否描述所有实现模块的安全功能要求相关接口、接口的返回值、与其他模块间的相互作用及调用的接口;
4) 是否提供实现模块和子系统间的对应关系。

b) 预期结果：

开发者提供的信息应满足 GB/T 21053 7.2.1.3 中所述的要求。

7.2.1.4 实现表示

产品设计部分的测评方法如下：

a) 测评流程：

检查开发者提供的实现表示证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否通过软件代码、设计数据等实例详细定义产品安全功能；
2) 是否提供实现表示与产品设计描述间的对应关系。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.1.4中所述的要求。

7.2.2 指导性文档

7.2.2.1 操作用户指南

产品设计部分的测评方法如下：

a) 测评流程：

检查开发者提供的操作用户指南证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否描述用户能访问的功能和特权(包含适当的警示信息)；
2) 是否描述如何以安全的方式使用产品提供的可用接口,是否描述产品安全功能及接口的用户操作方法(包括配置参数的安全值);
3) 是否标识和描述产品运行的所有可能状态,包括操作导致的失败或者操作性错误；
4) 是否描述实现产品安全目的必需执行的安全策略。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.2.1中所述的要求。

7.2.2.2 准备程序

准备程序部分的测评方法如下：

a) 测评流程：

检查开发者提供的准备程序证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 是否描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤；

2) 是否描述安全安装产品及其运行环境必需的所有步骤。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.2.2中所述的要求。

7.2.3 生命周期支持

7.2.3.1 配置管理能力

配置管理能力部分的测评方法如下：

a) 测评流程：

检查开发者提供的配置管理能力证据,并检查开发者提供的信息是否满足内容和形式的所有要求:

1) 检查开发者是否为不同版本的产品提供唯一的标识;
2) 现场检查配置管理系统是否对所有的配置项作出唯一的标识,且是否对配置项进行了维护;
3) 检查开发者提供的配置管理文档,是否描述了对配置项进行唯一标识的方法;
4) **现场检查是否能通过自动化配置管理系统支持产品的生成,是否仅通过自动化措施对配置项进行授权变更;**
5) **检查配置管理计划是否描述了用来接受修改过的或新建的作为产品组成部分的配置项的程序;检查配置管理计划是否描述如何使用配置管理系统开发产品,现场核查活动是否与计划一致。是否描述与开发者交付程序相一致的安全接收所交付产品必需的所有步骤。**

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.3.1中所述的要求。

7.2.3.2 配置管理范围

配置管理范围部分的测评方法如下：

a) 测评流程：

检查开发者提供的配置管理范围证据,并检查开发者提供的信息是否满足内容和形式的所有要求:

1) 检查开发者提供的配置项列表是否包含产品、安全保障要求的评估证据和产品的组成部分及相应的开发者;
2) **检查开发者提供的配置项列表是否包含实现表示、安全缺陷报告、解决状态及相应的开发者。**

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.3.2中所述的要求。

7.2.3.3 交付程序

交付程序部分的测评方法如下：

a) 测评流程：

检查开发者提供的交付程序证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 现场检查开发者是否使用一定的交付程序交付产品;
2) 检查开发者是否使用文档描述交付过程,文档中是否包含以下内容:在给用户方交付系统的各版本时,为维护安全所必需的所有程序。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.3.3中所述的要求。

7.2.3.4 开发安全

开发安全部分的测评方法如下：

a) 测评流程：

检查开发者提供的开发安全证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 检查开发者提供的开发安全文档,该文档是否描述在系统的开发环境中,为保护系统设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施;
2) 现场检查产品的开发环境,开发者是否使用了物理的、程序的、人员的和其他方面的安全措施保证产品设计和实现的保密性和完整性,这些安全措施是否得到了有效地执行。现场检查开发者是否使用一定的交付程序交付产品。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.3.4中所述的要求。

7.2.3.5 生命周期定义

生命周期定义部分的测评方法如下：

a) 测评流程：

检查开发者提供的生命周期定义证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 现场检查开发者是否使用生命周期模型对产品的开发和维护进行的必要控制;
2) 检查开发者提供生命周期定义文档是否描述了用于开发和维护产品的模型。现场检查开发者是否使用一定的交付程序交付产品。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.3.5中所述的要求。

7.2.3.6 工具和技术

工具和技术部分的测评方法如下：

a) 测评流程：

检查开发者提供的工具和技术证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 现场检查开发者是否明确定义用于开发产品的工具;
2) 是否提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.3.6中所述的要求。

7.2.4 测试

7.2.4.1 测试覆盖

测试覆盖部分的测评方法如下：

a) 测评流程：

检查开发者提供的测试覆盖证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 检查开发者提供的测试覆盖文档,在测试覆盖证据中,是否表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的;
2) 检查开发者提供的测试覆盖分析结果,是否表明功能规范中的所有安全功能接口都进行了测

试。现场检查开发者是否使用一定的交付程序交付产品。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.4.1中所述的要求。

7.2.4.2 测试深度

测试深度部分的测评方法如下：

a) 测评流程：

检查开发者提供的测试深度证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 检查开发者提供的测试深度分析,是否说明了测试文档中所标识的对安全功能的测试,并 足以表明与产品设计中的安全功能子系统和实现模块之间的一致性;
2) 是否能证实所有安全功能子系统、实现模块都已经进行过测试。现场检查开发者是否使用一定的交付程序交付产品。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.4.2中所述的要求。

7.2.4.3 功能测试

功能测试部分的测评方法如下：

a) 测评流程：

检查开发者提供的功能测试证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求:

1) 现检查开发者提供的测试文档,是否包括测试计划、预期的测试结果和实际测试结果,检查 测试计划是否标识了要测试的安全功能,是否描述了每个安全功能的测试方案;
2) 检查期望的测试结果是否表明测试成功后的预期输出;
3) 检查实际测试结果是否表明每个被测试的安全功能能按照规定进行运作。场检查开发者是否使用一定的交付程序交付产品。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.4.3中所述的要求。

7.2.4.4 独立测试

独立测试部分的测评方法如下：

a) 测评流程：

检查开发者提供的测试集合是否与其自测系统功能时使用的测试集合相一致,以用于安全功能的抽样测试,并检查开发者提供的资源是否满足内容和形式的所有要求。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.4.4中所述的要求。

7.2.5 脆弱性评定

脆弱性评定部分的测评方法如下：

a) 测评流程：

从用户可能破坏安全策略的明显途径出发,按照安全机制定义的安全强度级别,对产品进行脆弱性分析;判断产品是否能抵抗中等型型攻击。

b) 预期结果：

渗透性测试结果应表明产品能抵抗中等型攻击。

7.2.6 代码安全

代码安全部分的测评方法如下：

a) 测评流程：

检查开发者提供的代码安全证据,并检查开发者提供的信息是否满足证据的内容和形式的所有要求，确认开发者采用了代码审计等方式，对 PKI 系统进行安全性测试并提供相关测试文档，确保 PKI 系统的代码安全。

b) 预期结果：

开发者提供的信息应满足GB/T 21053 7.2.6中所述的要求。

参 考 文 献

[1]GB/T 20281-2020 信息安全技术 防火墙安全技术要求和测试评价方法