ICS 35.030
CCS L 80

中华人民共和国国家标准

GB/T 21054—2023
代替 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

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

2023-03-17 发布　　2023-10-01 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

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 21054—2007相比，除结构调整和编辑性改动外，主要技术变化如下：

a) 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》；

b) 对范围的内容进行了修改(见第1章，2007年版的第1章)；

c) 调整修改了规范性引用文件(见第2章，2007年版的第2章)；

d) 增加了“概述”一章，对PKI系统通用的测评方法进行了描述(见第5章)；

e) 将2007年版的第5章评估内容调整至新增的第6章安全功能测评方法和第7章安全保障测评方法(见第6章和第7章，2007年版的第5章)；

f) 删除了2007年版中关于物理安全的测评方法，将其中“数据输入输出”中关于原发抗抵赖的测评方法调整为6.9“原发抗抵赖”(见6.9，2007年版的5.1.2、5.3.2、5.1.6和5.3.7)。

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：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、公安部第一研究所、成都卫士通信息产业股份有限公司、北京信安世纪科技股份有限公司、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、格尔软件股份有限公司、北京百度网讯科技有限公司、同智伟业软件股份有限公司、北京软件产品质量检测检验中心、天津南大通用数据技术股份有限公司、西安西电捷通无线网络通信股份有限公司、郑州信大捷安信息技术股份有限公司、华为技术有限公司、国网区块链科技(北京)有限公司、北京中电华大电子设计有限责任公司、中国电子科技集团公司第十五研究所、北京奇虎科技有限公司、北京创原天地科技有限公司、数安时代科技股份有限公司、中国信息通信研究院、亚数信息科技(上海)有限公司、广州市百果园信息技术有限公司、广州市网星信息技术有限公司、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、王蕊、陈妍、冯登国、顾健、邱梓华、李景华、亢洋、李谦、刘丽敏、张妍、刘玉岭、张立廷、傅大鹏、郑强、张宝欣、汪宗斌、寇春静、刘金华、李健、丁肇伟、王现方、韩长青、金健、孟祥振、毛巨辉、李琴、韩秀德、褚超、石竹玉、黄钰、董晶晶、唐占国、肖青海、周蔚林、王榕、魏一才、朱晓宇、钟清华、李达、刘为华。

本文件及其所代替文件的历次版本发布情况为：

——2007年首次发布为GB/T 21054—2007；

——本次为第一次修订。

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—2023 规定了 PKI 系统的安全测评方法，包括安全功能测评方法和安全保障要求测评方法。

本文件适用于 PKI 系统的安全测评。

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 20518—2018　信息安全技术　公钥基础设施　数字证书格式

GB/T 21053—2023　信息安全技术　公钥基础设施 PKI 系统安全技术要求

GB/T 25069　信息安全技术　术语

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—2023 和 GB/T 25069 界定的术语和定义适用于本文件。

4　缩略语

GB/T 21053—2023 界定的缩略语适用于本文件。

5　概述

本文件依据 GB/T 21053—2023 规定的 PKI 系统的安全级别及相应级别的安全技术要求，给出了对应的安全测评方法。

PKI 系统的典型框架、安全功能及安全级别划分见 GB/T 21053—2023 中第 5 章。对于基本级的 PKI 系统，依据本文件第 6 章和第 7 章中与基本级安全要求对应的测评方法进行测评；对于增强级的 PKI 系统，依据本文件第 6 章和第 7 章中与增强级安全要求对应的测评方法进行测评。完成所有安全要素测评后，所有测评结论均为“符合”的，可给出被测评 PKI 系统“符合相应安全等级”的测评结论。其他情况，测评结论应记为“不符合相应安全等级”。

本文件中，使用**“宋体加粗”**的文字表示增强级 PKI 系统在基本级 PKI 系统基础上增加的安全要求对应的测评方法。

6　安全功能测评方法

6.1　密钥管理通用要求测评方法

密钥管理通用要求部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
   1) 查看 PKI 系统的密钥管理方案并确认密钥管理功能的实现方式；
   2) 通过核对证明材料等方式，验证 PKI 系统的密钥管理功能实现中密码产品使用情况；
   3) 执行密钥生成操作的密钥有效期设置，验证 PKI 系统的有效期设置功能。
b) 预期结果：
   1) PKI 系统文档中规定了密钥管理方案，能够根据密钥管理方案提供对应的密钥管理功能；
   2) PKI 系统实现密钥管理功能时，密码产品的使用符合 GB/T 21053—2023 中 6.1 b)的要求；
   3) PKI 系统能提供密钥有效期设置功能，并在生成系统密钥和订户密钥时根据策略为密钥设置有效期。
c) 结果判定：
   实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2 系统密钥管理

6.2.1 密钥生成

系统密钥生成部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
   1) 执行系统密钥生成操作，验证 PKI 系统的系统密钥生成时密码产品的使用情况；
   2) **在执行密钥生成操作时，验证 PKI 系统的系统密钥生成时密码模块的使用情况；**
   3) 使用具有不同权限的用户执行系统密钥生成操作，验证 PKI 系统密钥生成操作中的权限验证功能；
   4) **在执行密钥生成操作时，验证 PKI 系统 CA 密钥生成过程的权限控制情况；**
   5) 查看 PKI 系统文档，验证其中是否明确规定了系统密钥生成方法。
b) 预期结果：
   1) PKI 系统的系统密钥生成过程密码产品的使用符合 GB/T 21053—2023 中 6.2.1 a)的要求；
   2) **PKI 系统的系统密钥生成过程密码产品的使用符合 GB/T 21053—2023 中 6.2.1 b)的要求；**
   3) PKI 系统能提供密钥生成操作的权限验证功能，在密钥生成时检查用户角色，防止未授权操作；
   4) **PKI 系统的权限验证功能能够确保只有多于一个管理员角色的用户同时进行操作时才能启动 PKI 系统的 CA 密钥生成过程；**
   5) PKI 系统文档明确规定了系统密钥生成方法。
c) 结果判定：
   实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.2 密钥存储

PKI 系统密钥存储部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
   1) 查看 PKI 系统存储系统密钥的设备或文件，验证 PKI 系统的系统密钥存储功能；
   2) **访问密钥存储设备，验证 PKI 系统的系统密钥存储阶段密码产品的使用情况；**
   3) **确认 PKI 系统 CA 签名私钥的存储方式；**
   4) 查看 PKI 系统文档，验证其中是否明确规定了系统密钥存储方法和密钥泄露时的应急处置措施。
b) 预期结果：
   1) PKI 系统能提供系统密钥存储功能，系统密钥的私钥和秘密密钥部分均以加密形式存储；
   2) **PKI 系统中各类系统密钥的存储方式及使用的密码产品符合 GB/T 21053—2023 中 6.2.2 b)的要求；**
   3) **PKI 系统 CA 签名私钥的存储符合 GB/T 21053—2023 中 6.2.2 c)的要求；**

4） PKI 系统文档明确规定了系统密钥的存储方法和密钥泄露时的应急处置措施。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.3 密钥传送与分发

PKI 系统密钥传送与分发部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 对已生成的系统密钥执行传送与分发操作，验证 PKI 系统部件密钥的传送与分发方式，以及相关的保护措施；

2） 在执行密钥传送与分发时，验证 PKI 系统用户密钥的传送与分发方式，以及相关的保护措施；

3） 在执行密钥传送与分发时，验证 PKI 系统 CA 公钥的分发方法，以及相关的完整性保护措施；

4） **验证 1)和 2)中加密程序密码产品的使用情况**。

b） 预期结果：

1） PKI 系统部件密钥发送到 PKI 系统部件中时，具有完整性保护措施，私钥和秘密密钥部分以加密形式直接发送；

2） PKI 系统用户密钥发送到 PKI 系统用户的证书载体中时，具有完整性保护措施，私钥和秘密密钥部分以加密形式直接发送；

3） PKI 系统能提供可行的 CA 公钥分发方法，并具有完整性保护措施；

4） **密码产品的使用符合 GB/T 21053—2023 中 6.2.3 d)的要求**。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.4 密钥导入导出

PKI 系统密钥导入导出部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 对已生成的系统密钥执行导入导出操作，验证 PKI 系统的系统密钥导入导出方式，以及相关的保护措施，例如：加密、权限控制等；

2） 在执行密钥导入导出时，验证 PKI 系统密钥的导入导出过程中，私钥和秘密密钥部分的加密情况；

3） **在执行密钥导入导出时，验证 PKI 系统密钥的导入导出过程中，PKI 系统用户密钥、系统部件密钥和 CA 签名私钥使用密码产品加密保护的情况**。

b） 预期结果：

1） 密钥导入或导出 PKI 系统时，采取了有效的措施，保证密钥的安全；

2） PKI 系统密钥的导入导出过程中，私钥和秘密密钥部分始终以加密形式存在；

3） **PKI 系统密钥的导入导出过程中，PKI 系统密钥使用的密码产品符合 GB/T 21053—2023 中 6.2.4 c)的要求**。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.5 密钥使用

PKI 系统密钥使用部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

对已生成的系统密钥执行加密、签名等密钥使用操作，验证 PKI 系统的密钥使用功能，以及相关的权限管理机制。

b） 预期结果：

PKI 系统能提供密钥使用权限管理功能，将 PKI 系统的系统密钥与正确实体相关联，并赋予相应的权限，对非授权实体的密钥使用操作能够予以拒绝。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.6 密钥备份

PKI 系统密钥备份部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 对 PKI 系统密钥执行密钥备份操作，验证 PKI 系统的 CA 签名密钥备份功能；
2) **选择 CA 系统密钥以外的系统密钥执行密钥备份操作，验证 PKI 系统除 CA 签名密钥外的系统密钥备份功能；**
3) **访问 PKI 系统存储系统密钥备份的设备或模块，验证 PKI 系统的系统密钥备份存储方式；**
4) **访问 PKI 系统存储 CA 密钥备份的设备或模块，验证 PKI 系统 CA 签名私钥备份存储时的加密情况；**
5) **查看 PKI 系统文档，验证其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。**

b) 预期结果：

1) PKI 系统支持对 CA 签名密钥的备份功能；
2) **PKI 系统能够提供系统密钥备份功能，对 PKI 系统部件密钥和系统用户密钥进行备份；**
3) **PKI 系统密钥的备份存储符合 GB/T 21053—2023 中 6.2.6 c)的要求；**
4) **CA 签名私钥备份以加密形式存储，包含 CA 私钥信息的存放部件具备有效的访问控制机制，未授权情况下，无法访问存放部件；**
5) **PKI 系统文档明确规定了系统密钥的备份方法。**

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.7 密钥恢复

PKI 系统密钥恢复部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 执行 CA 签名密钥恢复操作，验证 PKI 系统的 CA 签名密钥恢复功能；
2) **选择 CA 签名密钥以外的密钥，执行密钥恢复操作，验证 PKI 系统的系统密钥恢复功能；**
3) 对作为备份存储的密钥执行密钥恢复操作，确认密钥恢复操作的权限控制机制；
4) **对作为归档存储的密钥执行密钥恢复操作，确认密钥恢复操作的权限控制机制；**
5) 在密钥恢复过程中，验证私钥和秘密密钥的加密情况；
6) **在 CA 签名私钥恢复过程中，验证人员权限确认和环境可信保护机制；**
7) 查看 PKI 系统文档，验证其中是否明确规定了密钥恢复方法。

b) 预期结果：

1) PKI 系统能够提供 CA 签名密钥恢复功能，允许必要时对 CA 签名密钥进行恢复，保证系统的可用性；
2) **PKI 系统能够提供系统密钥恢复功能，允许必要时对备份和归档的密钥进行恢复；**
3) 对于作为备份存储的密钥，只有密钥所有者能够执行密钥恢复操作；
4) **对于作为归档存储的密钥，PKI 系统在恢复密钥前能够验证申请者的身份，只有具有相应权限的实体能够执行密钥恢复操作；**
5) 密钥恢复过程中，私钥和秘密密钥以加密形式存在，且无法被未授权地泄露或修改；
6) **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，只有多个被授权的人同时使用存有密钥信息的部件才能进行，恢复环境安全可信，不危及密钥信息的安全性或暴露签名私钥，分布式方案的使用符合 GB/T 21053—2023 中 6.2.7 f)的要求；**

7） 对于支持密钥恢复的系统密钥，PKI 系统文档明确规定了系统密钥的恢复方法。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.8 密钥归档

6.2.8.1 私钥归档

PKI 系统密钥私钥归档部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 对 PKI 系统密钥私钥执行归档操作，验证 PKI 系统的系统密钥私钥归档功能，验证私钥归档的安全保护措施；

2） 分析密钥归档记录，验证 PKI 系统对归档密钥类型的区分情况；

3） **查看 PKI 系统文档，验证其中是否明确规定了 PKI 系统密钥的私钥归档方法，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。**

b） 预期结果：

1） PKI 系统的系统密钥私钥归档功能符合 GB/T 21053—2023 中 6.2.8.1 a)的要求，在私钥归档时具备有效的安全保护措施，防止私钥泄露；

2） PKI 系统能够区分用于签名的私钥和用于解密数据的私钥，确保签名私钥不能被归档；

3） **PKI 系统文档明确规定了系统密钥的归档方法。**

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.8.2 公钥归档

PKI 系统密钥公钥归档部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） **对 PKI 系统密钥私钥执行归档操作，验证 PKI 系统的公钥归档功能；**

2） **查看 PKI 系统文档，验证其中是否明确规定了 PKI 系统密钥的公钥归档方法，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。**

b） 预期结果：

1） **PKI 系统能够提供系统密钥的公钥归档功能，在数字证书从目录中移除后，支持通过归档的密钥验证数字签名；**

2） **PKI 系统文档明确规定了系统密钥的公钥归档方法。**

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.9 密钥销毁

PKI 系统密钥销毁部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） **对已生成的 PKI 系统密钥执行销毁操作，验证 PKI 系统的密钥销毁功能，确认密钥销毁方式以及过程中的权限验证机制；**

2） **对 CA 签名私钥执行销毁操作，确认 CA 签名私钥的销毁方式以及过程中的权限验证机制；**

3） 查看 PKI 系统文档，验证其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。

b） 预期结果：

1） **PKI 系统能够提供系统密钥的密钥销毁功能，密钥销毁方法具有不可逆性，并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；**

2） **CA 签名私钥的密钥销毁只有多个管理员同时在场才能执行，销毁过程包括多道销毁程序；**

3） PKI 系统支持系统密钥的密钥销毁功能，并在文档中明确规定了系统密钥的销毁方法。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.2.10 密钥更新

PKI 系统密钥更新部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 对已生成的 PKI 系统密钥执行密钥更新操作，验证 PKI 系统中系统密钥的更新功能；

2） **在密钥更新过程中，依据 6.2.1 中的测试方法对 CA 密钥及证书更新中新密钥对的生成进行测评；**

3） **在密钥更新过程中，依据 6.2.3 中的测试方法对 CA 密钥及证书更新中新公钥的分发进行测评；**

4） **在密钥更新过程中，依据 6.2.8 中的测试方法对 CA 密钥及证书更新中旧密钥对的归档进行测评；**

5） **在密钥更新过程中，依据 6.2.9 中的测试方法对 CA 密钥及证书更新中旧私钥的销毁进行测评；**

6） **查看 PKI 系统文档，验证是否对 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，验证相关措施是否在 PKI 系统中得到了实施；**

7） **查看 PKI 系统文档，验证其中是否明确规定了 CA 密钥及证书的更新方法，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。**

b） 预期结果：

1） PKI 系统能够提供系统密钥的密钥更新功能；

2） **新密钥对的生成的预期结果与 6.2.1 一致；**

3） **新公钥的分发的预期结果与 6.2.3 一致；**

4） **旧密钥对的归档的预期结果与 6.2.8 一致；**

5） **旧私钥的销毁的预期结果与 6.2.9 一致；**

6） **PKI 系统文档中对保障 CA 密钥更新时 PKI 系统服务的安全性和连续性的措施进行了说明，相关措施在 PKI 系统中得到了实施；**

7） **PKI 系统文档明确规定了 CA 密钥及证书的更新方法。**

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3 订户密钥管理

6.3.1 概述

根据 GB/T 21053—2023，PKI 系统的订户密钥包括订户签名密钥对和用于实现保密性保护的密钥对。本文件的 6.3.2～6.3.11 给出了订户密钥管理的测评方法。

6.3.2 密钥生成

订户密钥生成部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） **执行订户密钥生成操作，验证 PKI 系统订户签名密钥的生成方式；**

2） **在执行订户密钥生成操作时，验证 PKI 系统为订户密钥生成提供的相关机制；**

3） 执行订户密钥生成操作，验证 PKI 系统是否提供订户密钥生成功能，查看 PKI 系统文档，验证其中是否明确规定了订户密钥生成方法。

b） 预期结果：

1） **PKI 系统订户的签名私钥由其自己生成；**

2） **PKI 系统能够提供订户密钥生成相关机制，确保订户密钥生成符合 GB/T 21053—2023 中 6.3.2 b)的要求；**

3） PKI 系统能提供订户密钥生成功能，并在文档中明确规定了订户密钥生成方法。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.3 密钥存储

订户密钥存储部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） **查看 PKI 系统存储订户密钥的设备或文件，验证 PKI 系统的订户私钥在存储时的加密机制和密码产品使用情况；**

2） 查看 PKI 系统存储订户密钥的设备或文件，验证 PKI 系统是否提供了订户密钥存储功能。查看 PKI 系统文档，验证其中是否明确规定了订户密钥存储方法和密钥泄露时的应急处置措施。

b） 预期结果：

1） **PKI 系统的订户私钥存储符合 GB/T 21053—2023 中 6.3.3 a)的要求；**

2） PKI 系统能够提供订户密钥存储功能，PKI 系统文档明确规定了订户密钥的存储方法和密钥泄露时的应急处置措施。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.4 密钥传送与分发

订户密钥传送与分发部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 执行订户密钥传送与分发操作，验证 PKI 系统的订户密钥传送与分发功能，对于由订户自己生成的密钥，验证订户向 CA 提交密钥时的完整性保护机制；

2） 在订户密钥传送与分发操作过程中，对于订户委托 CA 生成的密钥，验证 CA 向用户传送与分发私钥时的机密性保护机制；

3） 查看 PKI 系统文档，验证其中是否明确规定了订户密钥传送方法。

b） 预期结果：

1） PKI 系统能提供订户密钥传送与分发功能。如果订户自己生成密钥对，PKI 系统能够接收订户向 CA 提交的密钥，并对订户公钥应用了完整性保护机制；

2） 如果订户委托 CA 生成密钥对，PKI 系统能够通过 CA 以加密形式向订户进行订户密钥传送与分发；

3） PKI 系统文档明确规定了订户密钥传送方法。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.5 密钥导入导出

订户密钥导入导出部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 对已生成的订户密钥执行密钥导入导出操作，确认 PKI 系统是否支持订户密钥导入导出，如果支持，验证 PKI 系统文档中关于订户密钥导入导出方法部分的规定；

2） 在密钥导入导出过程中，验证 PKI 系统是否能够提供订户密钥导入导出功能和相关安全措施；

3） 如果 PKI 系统支持订户密钥导入导出，则验证订户密钥导入导出过程中，私钥的加密情况。

b） 预期结果：

1） 如果 PKI 系统支持订户密钥导入导出，则 PKI 系统文档中规定了订户密钥导入导出方法；
2） 如果 PKI 系统支持订户密钥导入导出，则提供订户密钥导入导出功能并采取了有效的安全措施；
3） 如果 PKI 系统支持订户密钥导入导出，则 PKI 系统密钥的导入导出过程中，私钥始终以加密形式存在。

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.6 密钥使用

订户密钥使用部分的测试方法、预期结果和结果判定如下。

a） 测试方法：
对已生成的订户密钥执行加密、前面等密钥使用操作，验证 PKI 系统的密钥使用功能，以及相关的权限管理机制。

b） 预期结果：
PKI 系统能提供密钥使用权限管理功能，将 PKI 系统的订户密钥与正确实体相关联，并赋予相应的权限，对非授权实体的密钥使用操作能够予以拒绝。

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.7 密钥备份

订户密钥备份部分的测试方法、预期结果和结果判定如下。

a） 测试方法：
1） **查看 PKI 系统文档，验证其中是否规定了订户密钥备份方法，包括：密钥备份操作流程、采用的密钥备份方法等；**
2） **执行订户密钥备份操作，验证 PKI 系统的订户签名私钥的备份方式；**
3） **查看 PKI 系统中订户密钥的备份设备或文件，验证 PKI 系统订户加密密钥的备份情况，并验证由 PKI 系统进行备份的订户加密密钥的存储情况。**

b） 预期结果：
1） **PKI 系统文档明确规定了订户密钥的备份方法；**
2） **PKI 系统的订户签名私钥由用户自行备份；**
3） **如果 PKI 系统的订户加密密钥由 PKI 系统备份，则 PKI 系统能够提供系统密钥备份功能，订户密钥备份存储使用的密码产品符合 GB/T 21053—2023 中 6.3.7 c）的要求。**

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.8 密钥恢复

订户密钥恢复部分的测试方法、预期结果和结果判定如下。

a） 测试方法：
1） **执行订户密钥恢复操作，验证 PKI 系统的订户密钥恢复功能；**
2） **在密钥恢复过程中，验证私钥的加密情况；**
3） **如果 PKI 系统支持订户密钥恢复，查看 PKI 系统文档，验证其中是否规定了密钥恢复方法。**

b） 预期结果：
1） **如果 PKI 系统支持订户密钥备份，PKI 系统能够提供订户密钥恢复功能，允许必要时对由 PKI 系统备份的密钥进行恢复；**
2） **密钥恢复过程中，私钥信息以加密形式存在，且无法被未授权地泄露或修改；**
3） **如果 PKI 系统支持订户密钥恢复，则 PKI 系统文档规定了系统密钥的恢复方法。**

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.9 密钥归档

6.3.9.1 私钥归档

订户密钥私钥归档部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) **执行订户私钥归档操作，验证 PKI 系统的订户密钥归档功能；**
2) **分析密钥归档记录，验证 PKI 系统对归档密钥类型的区分情况；**
3) **查看 PKI 系统文档，验证其中是否规定了订户密钥的私钥归档方法，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。**

b) 预期结果：

1) **PKI 系统能够提供订户密钥归档功能，对需要被归档的私钥进行归档；**
2) **PKI 系统能够区分用于签名的私钥和用于解密数据的私钥，确保签名私钥不能被归档；**
3) **PKI 系统文档规定了订户密钥的归档方法。**

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.9.2 公钥归档

订户密钥公钥归档部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) **执行订户公钥归档操作，验证 PKI 系统的订户公钥归档功能；**
2) **查看 PKI 系统文档，验证其中是否明确规定了订户密钥的公钥归档方法，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。**

b) 预期结果：

1) **PKI 系统能够提供订户密钥的公钥归档功能，在数字证书从目录中移除后，支持通过归档的密钥验证数字签名；**
2) **PKI 系统文档明确规定了订户密钥的公钥归档方法。**

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.10 密钥销毁

订户密钥销毁部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) **执行订户密钥销毁操作，验证由 PKI 系统管理的订户密钥的销毁程序；**
2) 执行订户密钥销毁操作，验证 PKI 系统的订户密钥销毁功能，并查看 PKI 系统文档中是否规定了订户密钥销毁方法。

b) 预期结果：

1) **当由 PKI 系统管理的订户密钥被销毁时，订户密钥的销毁过程不可逆；**
2) PKI 系统支持订户密钥销毁，并在系统文档中规定了订户密钥的销毁方法。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.3.11 密钥更新

订户密钥更新部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) **对订户密钥执行密钥更新操作，依据 6.3.2 中的测试方法对订户密钥及证书更新中新密钥的生成进行测评；**

2) **在密钥更新过程中，依据 6.3.4 中的测试方法对订户密钥及证书更新中新密钥的分发进行测评；**
3) **在密钥更新过程中，依据 6.3.9 中的测试方法对订户密钥及证书更新中旧密钥对的归档进行测评；**
4) **在密钥更新过程中，依据 6.3.10 中的测试方法对订户密钥及证书更新中旧密钥的销毁进行测评；**
5) 对订户密钥执行密钥更新操作，验证 PKI 系统的订户密钥更新功能，查看 PKI 系统文档，验证是否对订户密钥更新时的安全性进行了明确说明；
6) **查看 PKI 系统文档，验证其中是否明确规定了订户密钥及证书的更新方法，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。**

b) 预期结果：
1) **新密钥的生成的预期结果与 6.3.2 一致；**
2) **新密钥的分发的预期结果与 6.3.4 一致；**
3) **旧密钥的归档的预期结果与 6.3.9 一致；**
4) **旧密钥的销毁的预期结果与 6.3.10 一致；**
5) PKI 系统支持订户密钥的密钥更新，在订户密钥更新时采取了安全措施保证订户密钥的安全性；
6) **PKI 系统文档明确规定了订户密钥及证书的更新方法。**

c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.4 模板管理

6.4.1 概述

根据 GB/T 21053—2023，在 PKI 系统中，可预先根据应用场景定义证书、CRL 和 OCSP 响应中字段和扩展可能的值，包含这些信息的数据称为模板。

6.4.2 证书模板管理

证书模板管理部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
1) 执行 PKI 系统的证书模板管理操作，验证 PKI 系统的证书模板管理功能及通过证书模板定义的证书中字段和扩展可能的值；
2) 执行证书颁发操作获取证书，验证证书的内容与证书模板的一致性；
3) 查看 PKI 系统发布的证书，验证 PKI 系统发布证书时，字段和扩展预先被指定的情况。

b) 预期结果：
1) PKI 系统能提供证书模板管理功能，管理员可通过证书模板预先定义证书中的字段和扩展可能的值，字段和扩展满足 GB/T 21053—2023 中 6.4.2 的要求；
2) PKI 系统能够确保发布的证书与证书模板中的描述一致；
3) PKI 系统发布证书时，GB/T 21053—2023 中 6.4.2 列出的字段和扩展的值均已预先被指定。

c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.4.3 证书撤销列表模板管理

证书撤销列表模板管理部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
1) 确定 PKI 系统是否发布 CRL，如果发布，执行 PKI 系统的 CRL 模板管理操作，验证 PKI 系统的 CRL 模板管理功能及通过 CRL 模板定义的证书中字段和扩展可能的值；

2） 执行 CRL 管理操作生成 CRL，验证 CRL 的内容与 CRL 模板的一致性；
3） 查看 PKI 系统发布的 CRL，验证 PKI 系统发布 CRL 时，字段和扩展预先被指定的情况。

b） 预期结果：
1） 如果 PKI 系统发布 CRL，则 PKI 系统能提供 CRL 模板管理功能，管理员可通过 CRL 模板预先定义 CRL 中的字段和扩展可能的值，字段和扩展满足 GB/T 21053—2023 中 6.4.3 的要求；
2） PKI 系统能够确保发布的 CRL 与 CRL 模板中的描述一致；
3） PKI 系统发布 CRL 时，GB/T 21053—2023 中 6.4.3 列出的字段和扩展的值均已预先被指定。

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.4.4 在线证书状态协议模板管理

在线证书状态协议模板管理部分的测试方法、预期结果和结果判定如下。

a） 测试方法：
1） 确定 PKI 系统是否发布 OCSP 响应，如果发布，执行 PKI 系统的 OCSP 模板管理操作，验证 PKI 系统的 OCSP 模板管理功能及通过 OCSP 模板定义的证书中字段和扩展可能的值；
2） 通过发送 OCSP 请求获取 OCSP 响应，验证 OCSP 响应的内容与 OCSP 模板的一致性；
3） 获取 PKI 系统发布的 OCSP 响应消息，验证 PKI 系统发布 OCSP 响应时，字段和扩展预先被指定的情况。

b） 预期结果：
1） 如果 PKI 系统发布 OCSP 响应，则 PKI 系统能提供 OCSP 模板管理功能，管理员可通过 OCSP 模板预先定义 OCSP 响应中的字段和扩展可能的值，字段和扩展满足 GB/T 21053—2023 中 6.4.4 的要求；
2） PKI 系统能够确保发布的 OCSP 响应与 OCSP 模板中的描述一致；
3） PKI 系统发布 OCSP 响应时，GB/T 21053—2023 中 6.4.4 列出的字段和扩展的值均已预先被指定。

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5 证书管理

6.5.1 通用要求

证书管理通用要求部分的测试方法、预期结果和结果判定如下。

a） 测试方法：
查看 PKI 系统文档中证书管理方法相关内容，并依据文档验证 PKI 系统的证书管理功能。

b） 预期结果：
PKI 系统文档中明确规定了验证证书管理方法，并提供了相应的证书注册、证书生成和证书撤销等证书管理功能。

c） 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5.2 证书注册

证书注册部分的测试方法、预期结果和结果判定如下。

a） 测试方法：
生成证书请求，提交至 PKI 系统执行证书注册流程，验证 PKI 系统对输入证书字段和扩展中的数据的校验和批准机制。

b） 预期结果：

PKI 系统能通过证书注册功能中实现对输入证书字段和扩展中的数据进行校验和批准，校验和批准方式符合 GB/T 21053—2023 中 6.5.2 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5.3 证书生成

证书生成部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 执行证书注册流程获取证书，检查 PKI 系统生成的证书，采用数字证书格式合规检测工具等验证其格式是否符合 GB/T 20518—2018 的要求；

2) 若 PKI 系统允许用户密钥对由用户生成，则由用户生成密钥对并执行证书请求，验证 PKI 系统对证书主体持有私钥的验证情况。

b) 预期结果：

1) PKI 系统生成的数字证书格式符合 GB/T 20518—2018 的要求；

2) 若 PKI 系统允许用户密钥对由用户生成，则 PKI 系统能够对证书主体拥有与证书中包含的公钥相对应的私钥进行验证，不持有与公钥对应的私钥情况下，证书注册请求无法完成。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5.4 证书撤销

6.5.4.1 采用证书撤销列表的证书撤销

采用证书撤销列表的证书撤销部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

确定 PKI 系统是否发布 CRL，如果发布，执行 CRL 发布操作并查看生成的 CRL 文件，验证 PKI 系统的 CRL 发布机制。

b) 预期结果：

如果 PKI 系统发布 CRL，则 PKI 系统能够提供 CRL 验证功能，对发布的 CRL 进行验证，确保发布的 CRL 的所有必要项的值符合 GB/T 20518—2018 中 5.3 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5.4.2 采用 OCSP 的证书撤销

采用 OCSP 的证书撤销部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

确定 PKI 系统是否发布 OCSP 响应，如果发布，通过发送 OCSP 请求的方式获取 OCSP 响应，并对获取到的 OCSP 响应消息进行查看，验证 PKI 系统的 OCSP 响应功能。

b) 预期结果：

如果 PKI 系统发布 OCSP 响应，则 PKI 系统能够提供 OCSP 响应验证功能，确保返回的 OCSP 响应的所有必要项的值符合 GM/T 0014—2012 中 5.6 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5.5 证书更新

证书更新部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 执行证书更新流程对已发布的订户证书进行更新，验证 PKI 系统的证书更新功能，并验证证

书更新时的密钥更新过程；

2） 执行 CA 证书更新流程对 CA 证书进行更新，验证 PKI 系统在此过程中服务的安全性和连续性；

3） 通过证书更新流程验证 PKI 系统的更新后证书的发布方式及其中的安全措施。

b） 预期结果：

1） PKI 系统支持证书更新功能，当证书更新中涉及密钥更新时，符合 6.2.10 和 6.3.11 中的安全要求；

2） CA 证书更新时，PKI 系统能够保证服务的安全性和连续性；

3） PKI 系统在发布更新后证书的过程中采取了相应的安全措施。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.5.6 证书变更

证书变更部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 执行证书变更流程，对已发布的证书中的部分信息进行变更，验证 PKI 系统的证书变更功能；

2） 验证 PKI 系统的变更后证书的发布方式及其中的安全措施。

b） 预期结果：

1） PKI 系统支持证书变更功能；

2） PKI 系统在发布变更后证书的过程中采取了相应的安全措施。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.6 身份鉴别

6.6.1 用户身份鉴别

用户鉴别部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 访问 PKI 系统，验证 PKI 系统的用户身份鉴别功能，并在不进行鉴别的情况下，执行与安全相关的操作，确认 PKI 系统的响应；

2） 在执行操作的过程中，验证 PKI 系统是否提供了安全无关操作的定义和相应处理机制；

3） 结合 PKI 系统的文档和登录过程中的实际操作，验证 PKI 系统支持的用户鉴别机制的定义和实现情况；

4） 在执行用户鉴别时，观察 PKI 系统的反馈，验证是否存在泄露用户鉴别数据的情况，例如：输入的口令被显示。

b） 预期结果：

1） PKI 系统能够提供用户身份鉴别功能，在用户执行动作时，对系统用户和订户进行身份鉴别；如果不进行鉴别或鉴别失败，则操作不能够被执行；

2） PKI 系统定义了适当的在标识用户前可由 PKI 系统代表用户执行的，与安全无关的动作；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） PKI 系统在文档中明确规定了所支持的用户鉴别机制的类型，并能够向用户提供支持的全部用户鉴别机制；

4） 用户鉴别时，PKI 系统的显示和操作不存在泄露用户鉴别数据的情况。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.6.2 多因素身份鉴别

多因素身份鉴别部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
   1) **访问 PKI 系统并执行多因素身份鉴别，确认 PKI 系统实现的鉴别机制，验证 PKI 系统对使用不同鉴别机制鉴别和多因素鉴别的支持情况；**
   2) **在进行身份鉴别时，验证多因素鉴别允许使用的鉴别机制组合的情况。**

b) 预期结果：
   1) **PKI 系统能够提供多因素身份鉴别机制，支持对不同身份的用户使用不同的鉴别机制，以及对同一用户同时使用多种鉴别过程进行多因素鉴别；**
   2) **对同一用户同时使用多种鉴别过程进行多因素鉴别时，所使用的鉴别机制中均包含基于数字证书的鉴别机制。**

c) 结果判定：
   实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.6.3 鉴别失败处理

鉴别失败处理部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
   1) 通过输入错误的口令、密钥等方式，执行失败的鉴别过程，验证 PKI 系统的鉴别失败检测功能；
   2) 执行鉴别机制的配置，验证 PKI 系统鉴别失败检测中参数配置情况；
   3) **验证 PKI 系统的鉴别失败处理功能。**

b) 预期结果：
   1) PKI 系统能够提供鉴别失败检测功能，当执行鉴别的失败次数达到预先设置的失败次数界限时，PKI 系统能够检测并记录此事件；
   2) PKI 系统能够提供鉴别失败检测参数配置功能，允许管理员配置失败的鉴别次数和失效时间值等参数；
   3) **PKI 系统能够提供鉴别失败处理功能，对检测到的鉴别失败事件采取应对措施，并保证至少有一个用户账号不应失效。**

c) 结果判定：
   实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.6.4 口令管理

口令管理部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
   1) 依据 PKI 系统文档执行口令管理操作，验证 PKI 系统口令管理中的安全机制；
   2) **执行由订户产生的订户鉴别口令生成操作，输入具有不同质量的口令，验证 PKI 系统对由订户自己产生的用户鉴别口令的强度检查情况；**
   3) **执行由系统产生的订户鉴别口令生成操作，查看生成的口令内容，验证 PKI 系统对由系统生成的用户鉴别口令的强度管理情况；**
   4) **验证 PKI 系统的口令使用期限管理功能。**

b) 预期结果：
   1) PKI 系统的口令管理安全机制符合 GB/T 21053—2023 中 6.6.4 a)的要求；
   2) **PKI 系统能够提供由订户自己产生的用户鉴别口令的强度检查功能，对可接受的口令的质量作出要求并检查；**
   3) **PKI 系统能够确保生成的用户鉴别口令强度满足 GB/T 21053—2023 中 6.6.4 c)的要求；**
   4) **PKI 系统能够提供口令使用期限管理功能，实现口令使用期限定义和定期更换。**

c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.7 访问控制

6.7.1 用户属性定义

用户属性定义部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
执行安全属性维护操作，验证 PKI 系统的安全属性维护功能。

b) 预期结果：
PKI 系统能够提供安全属性维护功能，允许管理员对用户的身份、组、角色、许可、安全和完整性等级等安全属性进行管理。

c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.7.2 角色与责任

角色与责任部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
1) 查看 PKI 系统文档，验证 PKI 系统文档中管理员和操作员角色定义情况和各角色的职责设置情况；
2) **验证 PKI 系统文档中审计员的角色定义情况及其职责设置情况；**
3) 执行用户管理操作，验证 PKI 系统提供的主体与角色关联功能，并确定 PKI 系统对角色管理的限制情况。

b) 预期结果：
1) PKI 系统在文档中提供了对系统管理员和操作员的角色定义，各角色的职责与 GB/T 21053—2023 中 6.7.2 a)无冲突；
2) **PKI 系统在文档中提供了对系统审计员的角色定义，审计员的职责与 GB/T 21053—2023 中 6.7.2 b)无冲突；**
3) PKI 系统能够提供主体与角色关联功能，并实现了对角色管理的限制，确保单个身份不应同时具备多个角色的权限，单个用户不应同时拥有多个角色。

c) 结果判定：
实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.7.3 系统用户访问控制

系统用户访问控制部分的测试方法、预期结果和结果判定如下。

a) 测试方法：
1) 执行系统用户管理操作，验证 PKI 系统的系统用户注册、注销功能，并确认对用户分配或者使用系统特权的操作进行的限制和控制情况；
2) **验证 PKI 系统的系统用户访问控制的用户权限审核机制；**
3) 使用系统用户执行相关操作，验证 PKI 系统对系统用户实施访问控制的情况；
4) **验证 PKI 系统文档中关键操作的定义和权限控制情况；**
5) 验证 PKI 系统文档中访问控制相关内容。

b) 预期结果：
1) PKI 系统能够提供系统用户注册、注销功能，并对用户分配或者使用系统特权的操作进行了严格的限制和控制；
2) **PKI 系统能够定期执行用户权限审核，审核系统用户的权限分配是否适当；**
3) PKI 系统能够提供系统用户访问控制功能，对系统用户的操作进行访问控制，阻止不符合访

问控制策略的系统用户操作执行；

4） **PKI 系统在文档中定义了关键操作，并通过访问控制功能确保当多个系统具有相应权限的用户同时通过身份鉴别后，才能执行相应的关键操作；**

5） PKI 系统在文档中包含访问控制文档相关内容，并涵盖了 GB/T 21053—2023 中6.7.3 e)中规定的相关内容。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.8 安全审计

6.8.1 审计数据产生

审计数据产生部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 执行 PKI 系统的审计管理操作，验证 PKI 系统的审计数据产生功能，并确定系统中维护的可审计事件；

2） **验证 PKI 系统维护的可审计事件对 GB/T 21053—2023 中 6.8.2 b)列出事件的涵盖情况；**

3） 执行可审计事件对应的操作，验证审计记录生成情况以及审计记录的内容；

4） 分析审计记录中私钥、对称密钥和其他安全相关的参数等敏感信息的加密情况；

5） 分析审计记录中可审计事件与发起该事件的用户身份关联的情况。

b） 预期结果：

1） PKI 系统能够提供审计数据产生功能，系统中已维护的所有可审计事件涵盖了 GB/T 21053—2023 中 6.8.2 a)规定的事件；

2） **PKI 系统维护的所有可审计事件涵盖了 GB/T 21053—2023 中 6.8.2 b)规定的事件；**

3） PKI 系统能够为每个可审计事件生成对应的审计记录，审计记录中包含的信息涵盖了 GB/T 21053—2023 中 6.8.2 c)规定的信息，内容与实际操作一致；

4） 审计记录中未出现明文形式的私钥、对称密钥和其他安全相关的参数；

5） 审计记录能够将可审计事件与发起该事件的用户身份进行了关联。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.8.2 审计查阅

审计查阅部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

执行 PKI 系统的审计记录查阅操作，验证 PKI 系统的审计记录查阅功能，并确认日志信息显示方式及适于阅读和解释的情况。

b） 预期结果：

PKI 系统能够提供审计记录查阅功能，管理员可通过该功能查看所有日志信息，日志信息的提供方式适于阅读和解释。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.8.3 选择性审计查阅

选择性审计查阅部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

执行选择性审计查阅操作，验证 PKI 系统安全审计功能中选择性审计查阅功能的情况以及返回的审计日志查阅结果与选择或排除的相关属性的一致性。

b） 预期结果：

PKI 系统能够提供选择性审计查阅功能，使管理员能够根据相关属性选择或排除审计事件集中的可审计事件；通过选择和排除特定类型的可审计事件并执行选择性审计查阅操作后，返回的审计日志查阅结果与选择或排除的相关属性一致。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.8.4 审计事件存储

审计事件存储部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 以未授权和授权形式对审计记录进行修改，验证 PKI 系统对审计记录修改的检测、记录和权限控制情况；

2) 将审计记录存储配置为已满状态，然后执行若干审计事件，验证 PKI 系统的审计记录防丢失功能。

b) 预期结果：

1) 以未授权形式对审计记录进行修改时，PKI 系统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；以授权形式对审计记录进行修改时，操作能够执行，PKI 系统能够检测到对审计记录的修改；

2) 审计记录存储配置为已满状态时，PKI 系统能够阻止由管理员发起的以外的审计事件的发生。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.8.5 审计日志完整性保护

审计日志完整性部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) **执行审计日志完整性保护配置操作，验证 PKI 系统对审计日志实施完整性保护机制的情况；**

2) **查看审计日志，分析完整性保护相关信息，并验证保护对象范围；**

3) **执行审计日志签名配置操作，验证完整性保护运算的时间周期配置情况；**

4) **查看审计日志，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。**

b) 预期结果：

1) **PKI 系统能够提供审计日志完整性保护功能，定期对审计日志使用密码技术进行完整性保护；**

2) **审计日志的完整性保护相关信息的保护对象（例如：数字签名对应的消息）中包含从上次运算后加入的所有审计日志条目以及上次完整性保护机制运算的结果；**

3) **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；**

4) **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。**

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.9 原发抗抵赖

原发抗抵赖部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) **执行原发抗抵赖机制配置操作，验证 PKI 系统的原发抗抵赖证据生成功能，确定原发抗抵赖令牌生成机制以及覆盖范围，验证 PKI 系统为安全信息生成的原发抗抵赖证据与信息原发者的关联性；**

2) **执行原发抗抵赖证据验证操作，验证 PKI 系统的原发抗抵赖证据验证功能。**

b) 预期结果：

1) **PKI 系统能提供原发抗抵赖令牌生成功能，采用密码技术保证证书状态信息以及其他安全信息的不可否认性；原发抗抵赖机制覆盖证书状态信息以及其他安全信息，原发抗抵赖证据中包含的信息与原发信息者正确关联；**

2) **PKI 系统能提供原发抗抵赖证据验证功能，对原发抗抵赖证据进行验证。**

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.10 备份和恢复

备份和恢复部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 执行 PKI 系统备份和恢复操作，验证 PKI 系统的备份和恢复功能的实现情况；

2) **查看 PKI 系统生成的备份数据，验证 PKI 系统备份数据的完整性和保密性保护机制；**

3) **分析 PKI 系统的备份方案是否能在不中断数据库使用的前提下实施；**

4) **分别将备份模式配置为人工和自动，并执行系统备份操作，验证 PKI 系统是否提供人工和自动备份模式；**

5) **分别将备份模式配置为实时和定期，并执行系统备份操作，验证 PKI 系统是否提供实时和定期备份模式；**

6) **将备份功能配置为增量模式，验证 PKI 系统是否提供增量备份功能；**

7) **执行 PKI 系统的归档检索操作，并选择检索到的归档记录执行恢复操作，验证 PKI 系统是否提供归档检索与恢复功能；**

8) **执行备份和恢复操作，观察操作过程中 PKI 系统的服务连续性，验证 PKI 系统对在线备份和恢复功能的支持。**

b) 预期结果：

1) PKI 系统能够提供备份和恢复功能；执行备份操作后，能够生成当前时间节点的系统备份数据，其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；

2) **PKI 系统通过数字签名等方式对备份数据进行了完整性保护，并对备份数据中的关键安全参数进行了加密；**

3) **PKI 系统能够提供在不中断数据库使用的前提下实施的备份方案；**

4) **PKI 系统能够提供人工和自动备份模式；**

5) **PKI 系统能够提供实时和定期备份模式；**

6) **PKI 系统能够提供增量备份模式；**

7) **PKI 系统能够提供归档检索与恢复功能；**

8) **PKI 系统支持通过在线备份和恢复等方式，能够在系统失败或者其他严重错误的情况下保证 PKI 系统服务的连续性。**

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.11 启动和运行检测

启动和运行检测部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

1) 执行 PKI 系统的初始化和启动操作，验证 PKI 系统在初始化、启动期间的启动监测功能的实现情况；

2) 执行 PKI 系统的运行监测管理操作，验证 PKI 系统运行期间的运行监测功能的实现情况。

b) 预期结果：

1) PKI 系统能够提供一定的启动监测功能，在初始化、启动期间对设备、组件和重要配置文件等进行检测，当发现异常时能够及时告警；

2） PKI 系统能够提供一定的运行监测功能，在系统运行期间对安全功能的运行情况进行检测，当出现异常时能够及时告警。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

6.12 组件间通信安全

组件间通信安全部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 在 PKI 系统各组件间部署通信监测工具，获取组件间通信内容，验证 PKI 系统各组件间通信安全机制的实现情况；

2） **访问 PKI 系统中实现组件间通信安全的模块或系统，验证 PKI 系统各组件间通信安全机制采用的密码产品和密码模块使用情况**。

b） 预期结果：

1） PKI 系统具备采用密码技术实现的组件间通信安全机制，保障 PKI 系统各组件间通信的保密性和完整性；

2） **PKI 系统各组件间通信安全机制实现时密码产品的使用符合 GB/T 21053—2023 中 6.12 b）的要求**。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7 安全保障要求测评方法

7.1 开发

7.1.1 安全架构

安全架构部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

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—2023 中 7.1.1 的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.1.2 功能规格说明

功能规格说明部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

检查开发者提供的功能规格说明证据，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—2023 中 7.1.2 的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.1.3 产品设计

产品设计部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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) **是否根据实现组件描述安全功能，是否描述所有实现组件的安全功能要求相关接口、接口的返回值、与其他组件间的相互作用及调用的接口；**
4) **是否提供实现组件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—2023 中 7.1.3 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.1.4 实现表示

实现表示部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.1.4 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.2 指导性文档

7.2.1 操作用户指南

操作用户指南部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.2.1 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.2.2 准备程序

准备程序部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.2.2 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.3 生命周期支持

7.3.1 配置管理能力

配置管理能力部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.3.1 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.3.2 配置管理范围

配置管理范围部分的测试方法、预期结果和结果判定如下。

a) 测试方法；

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—2023 中 7.3.2 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.3.3 交付程序

交付程序部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.3.3 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.3.4 开发安全

开发安全部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.3.4 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.3.5 生命周期定义

生命周期定义部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.3.5 的要求。

c) 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.3.6 工具和技术

工具和技术部分的测试方法、预期结果和结果判定如下。

a) 测试方法：

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—2023 中 7.3.6 的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.4 开发者测试

7.4.1 测试覆盖

测试覆盖部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

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格说明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，是否表明功能规格说明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—2023 中 7.4.1 中所述的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.4.2 测试深度

测试深度部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

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组件之间的一致性；

2） 是否能证实所有安全功能子系统、实现组件都已经进行过测试。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—2023 中 7.4.2 的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.4.3 功能测试

功能测试部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

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） 现场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。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—2023 中 7.4.3 的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.4.4 独立测试

独立测试部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

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—2023 中 7.4.4 的要求。

c） 结果判定：

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

7.5 脆弱性评定

脆弱性评定部分的测试方法、预期结果和结果判定如下。

a） 测试方法：

1） 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基本型攻击；

2） **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攻击**。

b） 预期结果：

1） 渗透性测试结果应表明产品能抵抗基本型攻击；

2） **渗透性测试结果应表明产品能抵抗中等型攻击**。

c） 结果判定

实际测评结果与相关预期结果一致则判定为符合，其他情况判定为不符合。

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
[2] GB/T 30270—2013 信息技术 安全技术 信息技术安全性评估方法

中 华 人 民 共 和 国
国 家 标 准
信息安全技术　公钥基础设施
PKI 系统安全测评方法
GB/T 21054—2023
*
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.spc.net.cn
服务热线:400-168-0010
2023 年 3 月第一版
*
书号:155066·1-72558

GB/T 21054-2023

码上扫一扫　正版服务到