测试项目A

密码应用方案

我

2022年09月02日

本页留白，便于双面打印。

编制说明

1. 本应用方案由项目建设单位组织编写并提交。
2. 编写要求：
   1. 语言规范、文字简练、重点突出、描述清晰、内容全面、附件齐全；
   2. 采用A4幅面，上、下、左、右边距均为2.5厘米；正文内容仿宋四号字，1.5倍行距；一级标题黑体三号字，二级标题楷体小三号字，三级标题仿宋四号字，各级标题均加黑；
   3. 涉及到的外文缩写要注明全称；
   4. 材料内容不得涉及国家秘密。
   5. 表格表头及内容，仿宋四号字，1倍行距。表头居中，表格左对齐

# 目 录

编制说明 I

目 录 I

1 项目背景 1

1.1 国家政策法规要求 2

1.2 密码应用现状 3

1.3 项目实施的必要性 3

2 系统概述 5

2.1 系统基本情况 5

2.2 物理和环境 6

2.3 网络和通信 6

2.3.1 网络拓扑 6

2.3.2 网络通信信道 7

2.4 设备和计算 7

2.5 应用和数据 9

2.5.1 业务应用 9

2.5.2 重要数据 10

2.6 管理制度 10

3 密码应用需求分析 11

3.1 通用需求分析 11

3.1.1 风险分析 11

3.1.2 密码应用需求 11

3.2 物理和环境 11

3.2.1 风险分析 11

3.2.2 密码应用需求 12

3.2.3 本系统需求分析清单-物理和环境 12

3.3 网络和通信 13

3.3.1 风险分析 13

3.3.2 密码应用需求 13

3.3.3 本系统需求分析清单-网络和通信 14

3.4 设备和计算 14

3.4.1 风险分析 14

3.4.2 密码应用需求 15

3.4.3 本系统需求分析清单-设备和计算 16

3.5 应用和数据 16

3.5.1 风险分析 16

3.5.2 密码应用需求 17

3.5.3 本系统需求分析清单-应用和数据 18

3.6 密钥安全管理 19

3.6.1 风险分析 19

3.6.2 密码应用需求 19

4 密码应用设计目标及原则 21

4.1 设计目标 21

4.2 设计原则 21

4.3 设计依据 22

5 密码应用技术方案 24

5.1 密码应用技术框架 24

5.2 物理和环境 27

5.2.1 密码应用技术方案 27

5.2.2 本系统密码应用技术方案-物理和环境 28

5.3 网络和通信 29

5.3.1 密码应用技术方案 29

5.3.2 本系统密码应用技术方案-网络和通信 30

5.4.1 密码应用技术方案 30

5.4 设备和计算 32

5.4.2 本系统密码应用技术方案-设备和计算 32

5.5 应用和数据 34

5.5.1 密码应用技术方案 34

5.5.2 本系统密码应用技术方案-应用和数据 35

5.6 密钥管理 37

5.6.1 密码应用技术方案 37

5.6.2 本系统密码应用技术方案-密钥管理 37

5.7 密码应用部署 39

5.8 密码软硬件产品 40

5.8.1 密码软硬件产品清单 40

5.8.2 密码软硬件产品介绍 42

5.9 安全与合规性分析 45

5.9.1 物理和环境 45

5.9.2 网络和通信 46

5.9.3 设备和计算 47

5.9.4 应用和数据 48

6 密码安全管理方案 50

6.1 管理制度 50

6.2 管理机构 51

6.3 建设运行 52

6.4 密钥管理 53

6.5 密码软硬件管理 54

6.6 人员管理 54

6.7 应急方案 55

6.7.1 潜在的安全事件分析 55

6.7.2 应急处置组织机构与职责 57

6.7.3 应急处置预案设计 59

7 实施保障方案 64

7.1 实施内容 64

7.1.1 软硬件开发及改造 64

7.1.2 系统集成 67

7.1.3 综合调试 68

7.1.4 试运行 68

7.1.5 最终验收 68

7.1.6 风险点及应对措施 68

7.2 实施计划 70

7.2.1 实施路线图 71

7.2.2 进度计划 71

7.3 保障措施 72

7.3.1 组织保障 73

7.3.2 人员保障 76

7.3.3 经费保障 76

7.3.4 质量保障 76

# 1 项目背景

密码技术作为网络与信息安全保障的核心技术和基础支撑，在身份认证、信息加密、安全隔离、完整性保护和操作抗抵赖等方面发挥着不可替代的作用。《国家信息化领导小组关于加强信息安全保障工作的意见》（中办发〔2003〕27号）提出“加强以密码技术为基础的信息保护和网络信任体系建设，要建立协调管理机制，规范和加强以身份认证、授权管理、责任认定等为主要内容的网络信任体系建设”。《国务院关于大力推进信息化发展和切实保障信息安全的若干意见》（国发〔2012〕23号）也提出“加强网络信任体系建设和密码保障，强化密码在保障电子政务、电子商务安全和保护公民个人信息等方面的支撑作用”。

2019年10月26日，十三届全国人大常委会第十四次会议通过《中华人民共和国密码法》，习近平主席签署主席令予以公布，于2020年1月1日起正式实施。密码法的出台，为密码科技实现跨越式发展、密码科技创新再上新台阶提供了宝贵的战略机遇和发展契机。当今以数字化、网络化、智能化为特征的信息技术日新月异，围绕5G、大数据、区块链等技术应用带来了大量的新的安全问题。密码技术是解决当前安全问题，保障信息安全最有效的关键核心技术。

2019年年底，国务院办公厅印发《国家政务信息化项目建设管理办法》，明确提出不符合密码应用和网络安全要求等情况的政务信息系统，不安排运行维护经费。项目建设单位应当落实国家密码管理有关法律法规和标准规范的要求，同步规划、同步建设、同步运行密码保障系统并定期进行评估。

2020年4月，国家发改委明确了“新基建”建设范畴。信息基础设施、融合基础设施、创新基础设施3个方面被纳入新型基础设施范畴。新型基础设施是以新发展理念为引领，以技术创新为驱动，以信息网络为基础，面向高质量发展需要，提供数字转型、智能升级、融合创新等服务的基础设施体系。

2021年3月9日，《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）正式发布，并于2021年10月1日起实施。“基本要求”从行业标准上升为国家标准，是**商用密码应用与安全性评估工作的重要里程碑。**

## 1.1 国家政策法规要求

1. 《中华人民共和国网络安全法》；
2. 《中华人民共和国密码法》；
3. 2018年7月中央办公厅印发的《金融和重要领域密码应用与创新发展工作规划（2018-2022)》；
4. 《信息安全技术 信息系统密码应用基本要求》（GB/T 39786-2021）；
5. 《信息安全技术网络安全等级保护基本要求》（GB/T 22239-2019）；
6. 《信息安全技术网络安全等级保护设计技术要求》（GB/T 25070-2019）；
7. 《中华人民共和国电子签名法》；
8. 《关键信息基础设施安全保护条例（征求意见稿）》；
9. 《网络安全等级保护条例（征求意见稿）》；
10. 《关于贯彻落实网络安全等级保护制度和关键信息基础设施安全保护制度的指导意见》；
11. 《商用密码应用安全性评估管理办法（试行）》；
12. 《金融和重要领域密码应用与创新发展工作规划（2018-2022年）》 厅字【2018】36号；
13. 《国家政务信息化项目建设管理办法》国办发【2019】57号；
14. 《国家密码管理局关于请进一步加强国家政务信息系统密码应用与安全性评估工作的函》国密局函【2020】119号；

## 1.2 密码应用现状

测试项目A平台在设计初期在网络通信方面传输通道未采取数据保密性措施;设备计算安全方面通过账号口令登录操作系统系统进行运维管理；在应用数据方面使用账号口令或动态验证密码实现应用登录验证；应用数据未使用加密技术加密存储。测试项目A平台整体现状未涉及商用密码安全应用。

如何合规、正确、有效使用商用密码，充分发挥商用密码在保障网络安全的核心技术和基础支撑作用，关乎国家大局、关乎网络空间安全、关乎用户隐私，然而当前密码安全形势严峻，商用密码应用现状不容乐观，主要存在密码应用不广泛、密码应用不规范和密码应用不安全等问题。

测试项目A密码应用建设充分考虑建立健全网络和信息系统密码保障体系的必要性，完善密码基础设施，提升密码适用管理水平，推进密码在重要领域系统身份认证、安全隔离、信息加密、信息数据保护等方面的应用，实现密码应用安全工作全面展开迫在眉睫。

## 1.3 项目实施的必要性

为贯彻落实《密码法》关于信息系统密码应用的要求，结合《国家电子政务建设指导意见》，决定对测试项目A进行密码应用方案设计，进一步加强重要基础设施的安全防范能力，提高运行保障水平，确保重要信息系统安全稳定运行，防止敏感信息泄露。

通过对测试项目A的现状和密码应用需求进行分析，依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》设计密码应用方案。

在网络安全上升到国家安全层面之后，测试项目A安全性要求，就成为了重中之重。测试项目A安全隐患主要分为两个层面：一是系统的安全，包括设备主机安全、中间件安全、操作系统安全、网络安全、应用安全等；二是数据的安全，在数据聚集化的趋势下，集中后的数据如何安全的存储、传输和使用也是个挑战。商用密码对于网络空间技术领域具有重要的基础性、引领性、关键性地位，特别是在数据加密、身份鉴别、访问控制、取证溯源等方面依然发挥着难以替代的重要作用。

到目前为止，密码技术仍是保障网络与信息安全最有效、最可靠、最经济的关键核心技术。通过基于密码技术的身份鉴别、信任管理、访问控制、数据加密、可信计算、密文计算、数据脱敏等措施，可以有效解决数据产生、传输、存储、处理、分析、使用等全生命周期安全问题，解决基础网络资源、信息设施、计算分析、应用服务、网络接入等全体系安全问题。

目前国际上通用的密码算法存在安全隐患，如RSA会被植入后门等，且使用的芯片大部分都是国外产品和技术，在我国尚未完成对这些核心技术控制的现状下，采用国产自主密码技术保障系统安全也成为必然的选择。

《中华人民共和国网络安全法》、《中华人民共和国密码法》（2020年1月1日正式施行）、《网络安全等级保护条例》的陆续颁布，及中央、地方的政策加强，进一步奠定了密码技术作为网络安全保护重要手段的地位。

因此，本项目的建设将切合国家网络安全政策要求，同时将有力地消除密码安全隐患，提升业务系统综合防护能力，保护国家和公共利益。

2 系统概述

首先要确认密码应用的目标信息系统对象，原则上和网络安全等级保护确定的对象、级别一致，分为1-4级，可参考《GBT 22240-2020信息安全技术—网络安全等级保护定级指南》确定目标信息系统，基本原则是1）具有确定的主要安全责任主体；2）承载相对独立的业务应用；3）包含相互关联的多个资源，避免将单个系统组件，如服务器、终端或网络设备作为对象。

根据对目标信息系统的调研整理系统情况，为后续风险分析、密码应用需求、方案设计奠定基础。2.1节介绍系统基本情况，根据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，2.2-2.5节分别介绍目标信息系统的物理和环境、网络和通信、设备和计算、应用和数据情况，2.6节介绍目前的密码管理制度。

2.1 系统基本情况

本小节介绍该系统的基本情况，包括系统名称、网络安全保护等级、等基本情况调研如表2.1所示：

表2.1 系统基本情况表

|  |  |  |  |
| --- | --- | --- | --- |
| 系统名称 | 测试项目A | 责任单位 | 我 |
| 系统建设 | 未建设 | 等保级别 | 三级 |
| 密评首次 | 首次 | 密码制度 | 未建设 |
| 云上部署 | 在云上 | 若在云上 | 云平台已过密评 |
| 服务端 | HTTPS | | |
| 移动端 | 无 | | |

系统用户情况调研如表2.2所示：

表2.2 系统用户表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 业务应用 | 用户/角色 | 登录方式 | 身份认证方式 | 所在网络 | 数量 |
| 业务A | 运维人员 | PC浏览器 | 手机短信, 用户名+口令 | 互联网 | 1 |
| 业务A | 系统管理员 | 手机APP | U盘证书 | 专网 | 1 |
| 业务A | 普通用户 | PC浏览器, PC客户端 | 手机短信, 用户名+口令 | 政务外网 | 1 |
| 业务A | 公众用户 | 微信小程序 | U盘证书, 用户名+口令 | 互联网 | 1 |

2.2 物理和环境

该信息系统涉及如表2.3所示机房：

表2.3 物理和环境调查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 机房名称 | 机房类型 | 门禁 | 身份认证方式 | 视频监控 | 是否允许增加设备 |
| 机房AADDDW | 新机房 | 普通电子 | 用户名+口令, IC卡 | 普通 | 是 |

2.3 网络和通信

2.3.1 网络拓扑

该系统网络拓扑，如图2.1所示：

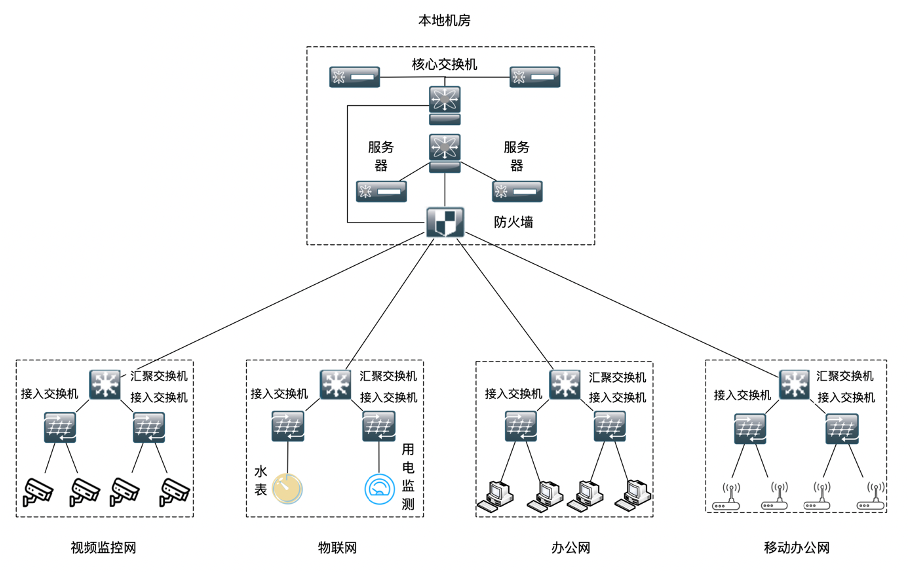


图 2.1 网络拓扑图

2.3.2 网络通信信道

本节介绍该系统的跨网络访问的通信信道情况如表2.4所示：

表2.4 网络和通信调查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 网络类型 | 通信主体 | 身份认证方式 | 是否涉及重要数据传输 | 数量/  流量 | 说明 |
| 互联网 | 运维人员 | 用户名+口令, U盘证书 | 是 | 10MBps | 撒旦法 |
| PC浏览器 | U盘证书, 用户名+口令 | 是 | 10MBps |  |
| PC-客户端 | 用户名+口令 | 是 | 10MBps | 撒旦法 |
| 移动APP | 用户名+口令 | 是 | 10MBps |  |
| 微信小程序 | 手机短信 | 否 | 10MBps | 撒旦法 |
|  | | | | |
| 办公局域网 | 运维人员 |  | 否 | 10MBps |  |
| PC浏览器 | 直接访问，无需认证 | 是 | 10MBps | 撒旦法 |
| PC-客户端 | 手机短信 | 是 | 10MBps | 撒旦法 |
| 移动APP | 邮箱验证 | 否 | 10MBps | 撒旦法 |
| 微信小程序 | 邮箱验证, 直接访问，无需认证 | 是 | 10MBps | 撒旦法 |
|  | | | | |

2.4 设备和计算

本节介绍该系统的软硬件设备情况如表2.5所示：

表2.5 通用设备调查表

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 设备名称 | 品牌型号 | 数量 | 操作系统 | 数据库 | 支持远程运维 | 运维人身份认证 | 通过堡垒机管理 |
| WWEQRW得到的 | dqwdwqdwq | 1 | Linux | Oracle | 是 | U盘证书, 用户名+口令 | 是 |

本节介绍该系统的其他软硬件设备情况如表2.6所示：

表2.6 专用设备调查表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 设备类型 | 设备名称 | 品牌型号 | 数量 | 是否支持国密算法 | 是否有商密证书 | 是否支持远程运维 | 身份认证方式 | 是否过堡垒机 |
| 密码产品/  密码设备 | 无 |  |  |  |  |  |  |  |
|  | | | | | | | |
| 具有密码功能的网络及安全设备(含云平台提供的虚拟VPN、堡垒机等) | SSL VPN | AKDDKw | 1 | 是 | 是 | 是 | 手机短信, U盘证书 | 否 |
| IPsec VPN | AKDDKwAKDDKw | 1 | 是 | 是 | 是 | 用户名+口令, U盘证书 | 是 |
| 堡垒机 | AKDDKwAKDDKw | 1 | 是 | 是 | 是 | 用户名+口令, U盘证书 | 是 |
|  | | | | | | | |
| 采用密码技术的其他产品 | 无 |  |  |  |  |  |  |  |
|  | | | | | | | |
| 没有密码功能的网络及安全设备 | 无 |  |  |  |  |  |  |  |
|  | | | | | | | |
| 虚拟设备和系统 | 无 |  |  |  |  |  |  |  |
|  | | | | | | | |

2.5 应用和数据

2.5.1 业务应用

本小节介绍系统所具有的功能及业务应用，如表2.7所示：

表2.7 业务应用调查表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 业务应用 | 功能描述 | 对外服务方式 | 操作需要不可否认性 | 具体情况 | 需要电子签名&电子印章 | 具体情况 |
| 业务A | 功能AAAAAA | HTTPS | 没有需求 | eqwewqewqewqewqewqeqw | 没有需求 | dmwqfjqwnfkqwqwdqw |

2.5.2 重要数据

该系统的重要数据如表2.8所示：

表2.8 重要数据调查表

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | 数据类型 | 数据内容 | 存储加密 | 数据量 | 传输加密 | 流量 |
| 业务A | 鉴别数据 | 但发觉我去你家请问你把钱弄完饭就去我那 | 国密 | 10Mb | 不涉及 | 10Mbps |
| 业务A | 重要业务数据 | 但发觉我去你家请问你把钱弄完饭就去我那 | 国密 | 10Mb | 不涉及 | 10Mbps |
| 业务A | 重要审计数据 | 但发觉我去你家请问你把钱弄完饭就去我那 | 国密 | 10Mb | 不涉及 | 10Mbps |
| 业务A | 个人敏感信息 | 但发觉我去你家请问你把钱弄完饭就去我那 | 国密 | 10Mb | 不涉及 | 10Mbps |
| 业务A | 法律法规规定的其他重要数 | 但发觉我去你家请问你把钱弄完饭就去我那 | 国密 | 10Mb | 不涉及 | 10Mbps |
| 业务A | 访问控制信息 | 但发觉我去你家请问你把钱弄完饭就去我那 | 非国密 | 10Mb | 不涉及 | 10Mbps |

2.6 管理制度

系统目前人员管理制度（岗位责任制度、人员考核制度、人员培训制度、关键岗位人员保密制度和关键岗位人员调离制度等）、建设运行、应急处置等制度并不完善。由于现有管理制度并不健全，将按照第6章密码安全管理方案进行改进。

3 密码应用需求分析

根据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，3.1节进行基本的、通用的风险分析，整理密码应用需求，3.2-3.5节分别从物理和环境、网络和通信、设备和计算、应用和数据四个方面进行风险分析，整理密码应用需求，并结合第2章目标信息系统的实际情况，分析出该系统每部分的密码应用需求清单，3.6节进行密钥的风险分析，并整理密钥管理需求。

3.1 通用需求分析

3.1.1 风险分析

对所有实现密码运算和密钥管理的密码产品，查看它们的商用密码产品型号证书或认证证书，确认其是否符合密码应用方案中的选型；若密码应用方案中未选定具体产品指标或安全等级，测评人员应当确认其是否属于GM/T 0028-2014要求三级及以上的密码模块或硬件密码产品。

3.1.2 密码应用需求

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，选择适当的具有商用密码产品型号证书或认证证书的密码产品。

3.2 物理和环境

3.2.1 风险分析

* 1. 设备所在机房应使用密码技术对进入机房人员进行身份鉴别，否则存在非授权人员进入物理环境，对软硬件设备和数据进行直接破坏的风险；
  2. 设备所在机房应使用密码技术对电子门禁记录进行数据完整性保护，否则存在数据被篡改的风险。
  3. 设备所在机房应使用密码技术对视频监控记录进行数据完整性保护，否则存在数据被篡改的风险。

3.2.2 密码应用需求

* 1. 经过上述的风险分析，设备所在机房应部署符合GM/T 0036-2014 标准要求的密码产品，对进出机房人员进行身份鉴别；
  2. 经过上述的风险分析，设备所在机房应部署符合密码相关国家、行业标准要求的电子门禁系统，对电子门禁记录数据进行完整性保护。
  3. 经过上述的风险分析，设备所在机房应部署符合密码相关国家、行业标准要求的视频监控系统，对视频监控音像记录数据进行完整性保护。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性为高风险项，现有系统在高风险项层面不能满足要求，存在较大风险。

3.2.3 本系统需求分析清单-物理和环境

表3.1 测评对象表-物理和环境

|  |
| --- |
| 测评对象 |
| 机房AADDDW |

本项目需求分析清单如表3.2所示。

表3.2 密码应用需求分析表-物理和环境

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 结论 |
| 机房AADDDW | 身份鉴别 | 宜 | 高 | 适用 | 目前机房的电子门禁是不符合GM/T 0036要求的基于密码技术的电子门禁系统，未采用密码技术保证进出机房人员的身份鉴别 | 不符合 |
| 机房AADDDW | 电子门禁记录数据存储完整性 | 宜 | 中 | 适用 | 系统目前未采用合规的电子门禁系统，不符合GM/T 0036要求，未采用密码技术保证电子门禁系统进出数据记录的存储完整性 | 不符合 |
| 机房AADDDW | 视频监控记录数据存储完整性 | 宜 | 中 | 适用 | 目前机房未采用合规的国密视频监控系统，未采用密码技术保证视频监控系统视频监控数据的存储完整性 | 不符合 |

3.3 网络和通信

3.3.1 风险分析

(1) 系统现存通信信道未采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性。

(2) 系统现存通信信道未采用密码技术保证通信过程中数据的完整性。

(3) 系统现存通信信道未采用密码技术保证通信过程中重要数据的机密性。

(4) 系统现存通信信道未采用密码技术保证网络边界访问控制信息的完整性。

(5) 系统现存通信信道未采用密码技术对外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。

3.3.2 密码应用需求

(1) 系统应部署符合密码相关国家、行业标准要求的密码设备或产品对通信实体进行身份鉴别，保证通信实体身份的真实性。

(2) 系统应部署符合密码相关国家、行业标准要求的密码设备或产品保证通信过程中数据的完整性。

(3) 系统应部署符合密码相关国家、行业标准要求的密码设备或产品保证通信过程中重要数据的机密性。

(4) 系统应部署符合密码相关国家、行业标准要求的密码设备或产品保证网络边界访问控制信息的完整性。

(5) 系统应部署符合密码相关国家、行业标准要求的密码设备或产品对外部连接到内部网络的设备进行接入认证，确保接入的设备身份真实性。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未采用密码技术对通信实体进行身份鉴别，保证通信实体身份的真实性、未采用密码技术保证通信过程中重要数据的机密性为高风险项，现有系统在高风险项层面不能满足要求，存在较大风险。

3.3.3 本系统需求分析清单-网络和通信

表3.3 测评对象表-网络和通信

|  |  |  |
| --- | --- | --- |
| 途经不受保护的网络类型 | 通信主体 | 测评对象 |
| 互联网 | 运维人员 | 互联网运维人员与系统之间的通信信道 |
| 互联网 | PC浏览器 | 互联网PC浏览器与系统之间的通信信道 |
| 互联网 | PC-客户端 | 互联网PC客户端与系统之间的通信信道 |
| 互联网 | 移动APP | 移动端APP与系统之间的通信信道 |
| 互联网 | 微信小程序 | 互联网PC客户端与系统之间的通信信道 |
| 办公局域网 | 运维人员 | 办公内网运维人员与系统之间的通信信道 |
| 办公局域网 | PC浏览器 | 办公内网PC浏览器与系统之间的通信信道 |
| 办公局域网 | PC-客户端 | 互联网PC客户端与系统之间的通信信道 |
| 办公局域网 | 移动APP | 物联网设备与系统之间的通信信道 |
| 办公局域网 | 微信小程序 | 系统与其他业务系统之间的通信信道 |

表3.4 密码应用需求分析表-网络和通信

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 结论 |
| 互联网运维人员与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 互联网运维人员与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 互联网运维人员与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 互联网运维人员与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 互联网运维人员与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 互联网PC浏览器与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 互联网PC浏览器与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 互联网PC浏览器与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 互联网PC浏览器与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 互联网PC浏览器与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 移动端APP与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 移动端APP与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 移动端APP与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 移动端APP与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 移动端APP与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 不适用 | 此通信信道不涉及重要数据的传输 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 办公内网运维人员与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 办公内网运维人员与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 办公内网运维人员与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 不适用 | 此通信信道不涉及重要数据的传输 | 不适用 |
| 办公内网运维人员与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 办公内网运维人员与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 办公内网PC浏览器与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 互联网PC客户端与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 物联网设备与系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 物联网设备与系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 物联网设备与系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 不适用 | 此通信信道不涉及重要数据的传输 | 不适用 |
| 物联网设备与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 物联网设备与系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |
| 系统与其他业务系统之间的通信信道 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对通信实体进行身份鉴别 | 不符合 |
| 系统与其他业务系统之间的通信信道 | 通信数据完整性 | 宜 | 中 | 适用 | 未采用密码技术保证通信过程中数据的完整性 | 不符合 |
| 系统与其他业务系统之间的通信信道 | 通信过程中重要数据的机密性 | 应 | 高 | 适用 | 未采用密码技术保证通信过程中重要数据的机密性 | 不符合 |
| 系统与其他业务系统之间的通信信道 | 网络边界访问控制信息的完整性 | 宜 | 中 | 适用 | 未采用密码技术对边界访问控制信息的完整性进行保护 | 不符合 |
| 系统与其他业务系统之间的通信信道 | 安全接入认证 | 可 | 中 | 不适用 | 三级系统不作此需求 | 不适用 |

3.4 设备和计算

3.4.1 风险分析

* 1. 系统运维人员未通过安全访问服务设备、安全组件与系统建立连接，未使用密码技术对运维人员进行身份鉴别，存在设备被非授权人员登录风险。
  2. 系统运维人员远程管理设备时，未采用密码技术建立安全的信息传输通道，存在信息传输通道被未授权使用，或传输数据未授权被获取和篡改等风险。
  3. 系统中未采用密码技术对系统资源访问控制信息进行完整性保护，存在系统资源访问控制信息未授权被篡改的风险。
  4. 系统未采用密码技术保证设备中重要信息资源安全标记的完整性，存在设备中重要信息资源安全标记被非授权篡改风险。
  5. 系统未采用密码技术对应用服务器、数据库服务器等设备日志记录进行完整性保护，存在日志记录被非授权篡改风险。
  6. 系统未采用密码技术对重要可执行程序进行完整性保护，并对其来源进行真实性验证，存在重要可执行程序被非授权篡改、来源不可信风险。

3.4.2 密码应用需求

根据上述风险分析，有以下应用需求。

（1）应部署符合密码相关国家、行业标准要求的密码设备或产品，并针对运维人员提供相应密码技术产品或设备的支撑，对运维人员进行身份鉴别，防止非授权人员登录。

（2）应部署符合密码相关国家、行业标准要求的密码设备或产品，建立安全的信息传输通道，防止信息传输通道被非授权使用，或传输数据被非授权获取篡改。

（3）应部署符合密码相关国家、行业标准要求的密码设备或产品，对系统资源访问控制信息进行完整性保护，防止被非授权篡改。

（4）应部署符合密码相关国家、行业标准要求的密码设备或产品，对设备中的重要信息资源安全标记进行完整性保护。

（5）应部署符合密码相关国家、行业标准要求的密码设备或产品，对日志记录进行完整性保护。

（6）应部署符合密码相关国家、行业标准要求的密码设备或产品，对重要可执行程序进行完整性保护，并对其来源进行真实性验证。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性；远程管理设备时，未采用密码技术建立安全的信息传输通道为高风险项现有系统在高风险项层面不能满足要求，存在较大风险。

3.4.3 本系统需求分析清单-设备和计算

表3.5 测评对象表-设备和计算

|  |  |  |
| --- | --- | --- |
| 设备类型 | 设备 | 测评对象 |
| 通用设备 | WWEQRW得到的 | WWEQRW得到的 |
| 具有密码功能的网络及安全设备(含云平台提供的虚拟VPN、堡垒机等) | SSL VPN | SSL VPN |
| 具有密码功能的网络及安全设备(含云平台提供的虚拟VPN、堡垒机等) | IPsec VPN | IPsec VPN |
| 具有密码功能的网络及安全设备(含云平台提供的虚拟VPN、堡垒机等) | 堡垒机 | 堡垒机 |

表3.6 密码应用需求分析表-设备和计算

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状/不适用解释 | 结论 |
| WWEQRW得到的 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性 | 不符合 |
| WWEQRW得到的 | 远程管理通道安全 | 应 | 高 | 适用 | 未采用符合国家或密码行业要求的密码算法、密码技术 | 不符合 |
| WWEQRW得到的 | 系统资源访问控制信息完整性 | 宜 | 中 | 适用 | 未采用密码技术对系统访问控制信息的完整性进行保护 | 不符合 |
| WWEQRW得到的 | 重要信息资源安全标记完整性 | 宜 | 中 | 不适用 | 系统无重要信息资源安全标记 | 不适用 |
| WWEQRW得到的 | 日志记录完整性 | 宜 | 中 | 适用 | 未采用密码技术保证日志记录的完整性 | 不符合 |
| WWEQRW得到的 | 重要可执行程序完整性、重要可执行程序来源真实性 | 宜 | 中 | 适用 | 未使用密码技术实现可执行程序的完整性和来源的真实性 | 不符合 |
| SSL VPN | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性 | 不符合 |
| SSL VPN | 远程管理通道安全 | 应 | 高 | 适用 | 未采用符合国家或密码行业要求的密码算法、密码技术 | 不符合 |
| SSL VPN | 系统资源访问控制信息完整性 | 宜 | 中 | 适用 | 未采用密码技术对系统访问控制信息的完整性进行保护 | 不符合 |
| SSL VPN | 重要信息资源安全标记完整性 | 宜 | 中 | 不适用 | 系统无重要信息资源安全标记 | 不适用 |
| SSL VPN | 日志记录完整性 | 宜 | 中 | 适用 | 未采用密码技术保证日志记录的完整性 | 不符合 |
| SSL VPN | 重要可执行程序完整性、重要可执行程序来源真实性 | 宜 | 中 | 适用 | 未使用密码技术实现可执行程序的完整性和来源的真实性 | 不符合 |
| IPsec VPN | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性 | 不符合 |
| IPsec VPN | 远程管理通道安全 | 应 | 高 | 适用 | 未采用符合国家或密码行业要求的密码算法、密码技术 | 不符合 |
| IPsec VPN | 系统资源访问控制信息完整性 | 宜 | 中 | 适用 | 未采用密码技术对系统访问控制信息的完整性进行保护 | 不符合 |
| IPsec VPN | 重要信息资源安全标记完整性 | 宜 | 中 | 不适用 | 系统无重要信息资源安全标记 | 不适用 |
| IPsec VPN | 日志记录完整性 | 宜 | 中 | 适用 | 未采用密码技术保证日志记录的完整性 | 不符合 |
| IPsec VPN | 重要可执行程序完整性、重要可执行程序来源真实性 | 宜 | 中 | 适用 | 未使用密码技术实现可执行程序的完整性和来源的真实性 | 不符合 |
| 堡垒机 | 身份鉴别 | 应 | 高 | 适用 | 未采用密码技术对登录设备的用户进行身份鉴别，保证用户身份的真实性 | 不符合 |
| 堡垒机 | 远程管理通道安全 | 应 | 高 | 适用 | 未采用符合国家或密码行业要求的密码算法、密码技术 | 不符合 |
| 堡垒机 | 系统资源访问控制信息完整性 | 宜 | 中 | 适用 | 未采用密码技术对系统访问控制信息的完整性进行保护 | 不符合 |
| 堡垒机 | 重要信息资源安全标记完整性 | 宜 | 中 | 不适用 | 系统无重要信息资源安全标记 | 不适用 |
| 堡垒机 | 日志记录完整性 | 宜 | 中 | 适用 | 未采用密码技术保证日志记录的完整性 | 不符合 |
| 堡垒机 | 重要可执行程序完整性、重要可执行程序来源真实性 | 宜 | 中 | 适用 | 未使用密码技术实现可执行程序的完整性和来源的真实性 | 不符合 |

3.5 应用和数据

3.5.1 风险分析

* 1. 系统不能保证应用系统用户身份的真实性，应采用密码技术对登录用户进行身份鉴别。
  2. 系统中存在信息系统应用的访问控制信息被未授权篡改的风险，应采用密码技术保证信息系统应用的访问控制信息的完整性。
  3. 系统中存在信息系统应用的重要信息资源安全标记被未授权篡改的风险，应采用密码技术保证信息系统应用的重要信息资源安全标记的完整性。
  4. 系统应用的重要数据存在重要数据被窃取和非授权篡改风险，应使用密码技术进行传输机密性和完整性、存储机密性和完整性保护。
  5. 系统应采用密码技术实现数据原发行为的不可否认性和数据接收行为的不可否认性。

3.5.2 密码应用需求

（1）应在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，实现对登录用户的安全身份鉴别，保证应用系统用户身份的真实性。

（2）应在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，对信息系统应用的访问控制信息进行完整性保护，防止被非授权篡改。

（3）在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，对信息系统应用的重要信息资源安全标记进行完整性保护，防止被非授权篡改。

（4）应部署符合密码相关国家、行业标准要求的密码设备或产品，应用通过调用该密码设备或产品，对系统应用的重要数据进行传输机密性和完整性、存储机密性和完整性保护，实现重要数据防窃取和防篡改保护。

（5）应在密码基础设施区部署符合密码相关国家、行业标准要求的密码设备或产品，实现数据原发行为的不可否认性和数据接收行为的不可否认性。

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》，未采用密码技术对登录用户进行身份鉴别，保证应用系统用户身份的真实性；未采用密码技术保证信息系统应用的重要数据在传输过程中的机密性；未采用密码技术保证信息系统应用的重要数据在存储过程中的机密性；未采用密码技术保证信息系统应用的重要数据在存储过程中的完整；在可能涉及法律责任认定的应用中，未采用密码技术提供数据原发证据和数据接收证据，实现数据原发行为的不可否认性和数据接收行为的不可否认性为高风险项，现有系统在高风险项层面不能满足要求，存在较大风险。

3.5.3 本系统需求分析清单-应用和数据

表3.7 测评对象表-应用和数据

|  |  |
| --- | --- |
| 业务应用 | 测评对象 |
| 业务A | 业务A |
| 鉴别数据 | 重要数据 |
| 重要业务数据 | 重要数据 |
| 重要审计数据 | 重要数据 |
| 个人敏感信息 | 重要数据 |
| 法律法规规定的其他重要数 | 重要数据 |

表3.8 密码应用需求分析表-应用和数据

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 要求 | 风险等级 | 适用情况 | 系统现状 | 结论 |
| 业务A | 身份鉴别 | 应 | 高 | 适用 | 系统未采用合规的密码技术对登录用户进行身份鉴别 | 不符合 |
| 业务A | 访问控制信息完整性 | 宜 | 中 | 适用 | 系统中访问控制信息采用了国密技术进行完整性保护 | 符合 |
| 业务A | 重要信息资源安全标记完整性 | 宜 | 中 | 不适用 | 本系统不涉及重要信息资源安全标记 | 不适用 |
| 业务A | 重要数据传输机密性 | 应 | 高 | 不适用 | 本系统不涉及重要数据传输机密性 | 不适用 |
| 业务A | 重要数据存储机密性 | 应 | 高 | 不适用 | 系统已经采用了合规的密码技术进行了存储机密性的保护 | 不适用 |
| 业务A | 重要数据传输完整性 | 宜 | 中 | 不适用 | 本系统不涉及重要数据传输完整性 | 不适用 |
| 业务A | 重要数据存储完整性 | 宜 | 高 | 不适用 | 系统已经采用了合规的密码技术进行了存储机密性的保护 | 不适用 |
| 业务A | 不可否认性 | 宜 | 高 | 不适用 | 系统不需要保证不可否认性 | 不适用 |

3.6 密钥安全管理

本小节针对密码安全管理中存在的风险提出了对应的密码应用需求，如下。

3.6.1 风险分析

本系统建设阶段，未依据密码相关国家、行业标准，制定密码应用方案，规划建设密码保障系统，系统上线前和运行后，均未开展过密码应用安全性评估，未依据《基本要求》中的安全管理要求，制定密码相关管理制度，不利于落实密码相关国家政策要求，发挥密码在信息系统安全中的基础支撑作用。

3.6.2 密码应用需求

依据《基本要求》，制定本系统密码应用方案，并委托密评机构对密码应用方案进行评估，制定密码相关的管理制度，系统改造完成后，依据密码应用改造方案对本系统进行密码应用安全性评估，评估通过后，评估通过后上线运行。

4 密码应用设计目标及原则

根据《政务信息系统密码应用与安全性评估工作指南（2020版）》、《国家政务信息化项目建设管理办法》、《商用密码应用安全性评估管理办法（试行）》、《政务信息系统政府采购管理暂行办法》（财库〔2017〕210 号），信息系统无论在规划、建设、运行哪个阶段，项目建设单位和使用单位都应当开展商用密码应用与安全性评估工作。首要就是要撰写《密码应用方案》，密码应用方案是信息系统密码应用的起点，它直接决定着信息系统的密码应用能否合规、正确、有效地部署实施，密码应用方案也是开展信息系统密码应用情况分析和评估工作的基础条件，其设计需依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况进行设计，并遵循以下设计目标及原则。

4.1 设计目标

围绕《信息系统密码应用基本要求》标准要求，综合考虑测试项目A物理和环境、网络和通信、设备和计算、应用和数据、安全管理等层面的密码应用需求，设计合规、正确、有效的密码应用方案，满足《基本要求》中三级指标要求，并为通过密码应用安全性评估奠定基础。

4.2 设计原则

结合设计目标及相关法规的要求，测试项目A密码应用设计应遵循以下原则：

1. 全面考虑、重点部署、分步实施原则

测试项目A中重要的基础设施和关键信息系统，是融合设备、技术、管理于一体的系统工程，需要全面考虑。同时，要考虑到涉及信息系统安全的重点因素，充分考虑可扩展性和可持续性，从解决眼前问题、夯实基础、建设整个体系方面做好边密码应用工作。

1. 规范性、先进性、可扩展性、完整性并重原则

为保证系统管理工作的有效性和规范性，相关工作应按照国家有关标准实施。系统应采用成熟先进的技术，密码应用总体框架和密码产品必须有较强的可扩展性，为测试项目A改进和完善创造条件。

1. 经济性和适度性并重原则

测试项目A的建设需要综合考虑资产价值、风险等级，实现总体安全保障。坚持运用风险评估的方法，提出相应的改进措施，对重要基础设施和关键信息系统进行适度的安全建设。

1. 技术和管理并重原则

先进成熟的安全技术防护体系是信息系统稳定运行的必备前提，遵循电子政务信息化发展思路，依据相关国家及行业标准，实现技术体系建设和管理体系建设的有效融合，技术与管理双管齐下，协同发展，有效保障电子政务密码应用的可持续发展。

4.3 设计依据

测试项目A的设计主要依据的国家法律法规具体如下所示：

1. GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》
2. GM/T 0071-2019《电子文件密码应用指南》
3. GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
4. GM/T 0024-2014《VPN综合安全网关 技术规范》
5. GM/T 0025-2014《VPN综合安全网关 网关产品规范》
6. GM/T 0026-2014《安全认证网关产品规范》
7. GM/T 0030-2014《服务器密码机技术规范》
8. GM/T 0031-2014《安全电子签章密码技术规范》
9. GM/T 0027-2014《智能密码钥匙技术规范》
10. GM/T 0033-2014《时间戳接口规范》
11. GM/T 0014-2012《证书认证系统密码协议规范》
12. GM/T 0028-2014《密码模块安全技术要求》
13. GM/T 0029-2014《签名验签服务系统技术规范》
14. GW0013-2017《安全要求》
15. 《信息系统密码应用高风险判定指引》

5 密码应用技术方案

根据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况，项目预算及拟采购的密码产品，设计密码应用技术方案，保障密码应用的合规性、正确性和有效性。

其中，5.1节介绍密码应用技术框架和整体架构，5.2-5.5节分别从物理和环境、网络和通信、设备和计算、应用和数据四个方面介绍典型的密码应用技术方案，以及结合本系统实际情况、采用的密码产品、设计的密码应用解决方案，5.6节介绍密钥管理方案，5.7节介绍密码应用部署，5.8节介绍本项目拟采购的密码软硬件产品，5.9节从物理和环境、网络和通信、设备和计算、应用和数据四个方面，做商用密码应用的技术部分安全与合规性分析。

5.1 密码应用技术框架

基于国产密码标准体系和密码管理体系，结合目标信息系统的实际情况，基于GB/T 39786-2021《信息系统密码应用基本要求》，建设以保护业务系统的身份认证及数据资产为中心的、自主可控的密码服务体系，通过核心的密码技术、密码模块、密码产品、密码基础设施等产品服务，为网络基础资源、信息设施、计算分析、应用服务、网络通道、接入终端、设备控制等提供身份鉴别、访问控制、数据机密性、完整性、及抗抵赖的密码服务。

密码应用技术总体架构如图 5.1所示。



图 5.1 密码应用技术架构

密码应用技术框架分为密码基础服务层和密码应用层，密码应用层包括终端安全密码应用、网络接入安全密码应用、业务安全密码、平台管理安全密码应用四部分。

1. 密码基础服务层

密码基础服务层由服务器密码机、签名验签服务器、时间戳服务器、数字证书认证系统、安全电子签章系统、密钥管理系统等设备组成，通过统一密码服务中间件，为业务应用提供数据加密服务、时间戳服务、签名验签服务、完整性验证服务等密码应用所需基础服务。

1. 密码应用层

密码应用层通过调用密码服务平台的一系列服务来保证密码应用安全：

* 1. 终端安全密码应用：采用智能密码钥匙解决用户在登录系统和业务操作的身份鉴别，保证了身份的真实性。
  2. 网络接入安全密码应用，部署可信浏览器、IPSec VPN，实现终端身份鉴别和数据传输加密保护；在PC端部署VPN客户端，建立数据安全传输通道。
  3. 系统业务安全密码应用，主要为业务应用提供身份验证服务、数据加密服务、完整性验证服务、数据安全存储服务。

密码基础服务平台

基于各密码产品构建的密码基础服务平台的主要功能是为上层应用提供密码基础服务支撑，实现上层应用的密码安全增强。该平台使用符合国家密码法规和标准规定的商用密码算法，使用经过国家密码管理局核准的密码产品，遵循“GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》”以及相关“密评”规范。

密码基础服务平台整合服务器密码机、证书认证系统、签名验签服务系统、通用统一密码等产品能力，打造服务化、场景化，易于行业快速对接集成的密码服务能力，实现密码基础服务平台统一、集约化建设，密码服务按需获取，弹性扩展。

密码基础服务如图 5.2所示。

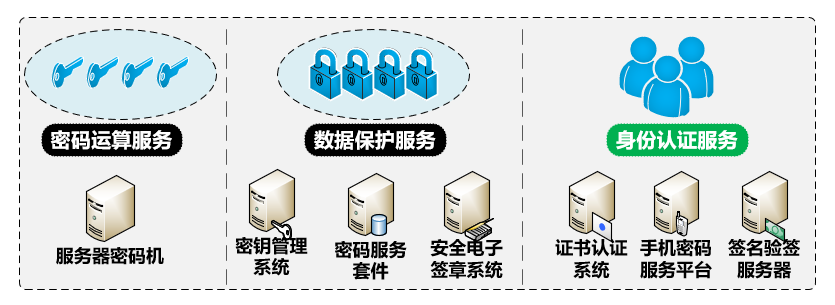


图 5.2 密码基础服务

5.2 物理和环境

5.2.1 密码应用技术方案

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》：采用基于密码技术的电子门禁系统和视频监控系统，对设备机房出入人员的身份进行鉴别，并对电子门禁系统进出记录数据和视频监控音像记录数据进行完整性保护。

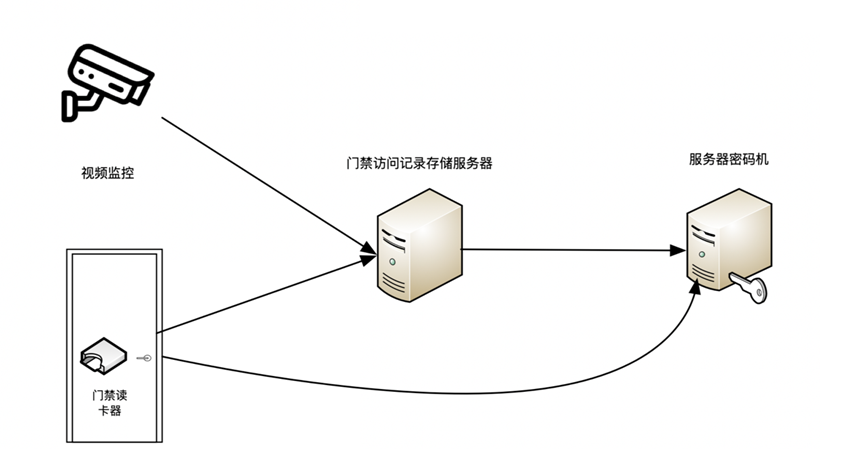


图 5.4 物理环境图

1. 身份鉴别：采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，保护物理访问控制身份鉴别信息。符合该标准的电子门禁系统使用SM4等算法进行密钥分散，实现门禁卡的一卡一密，并基于SM4等算法鉴别人员身份。
2. 电子门禁记录数据完整性：采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，电子门禁系统进出记录应严格进行完整性保护，完整的进出记录是实现安全管理、事后追责的重要基础。符合该标准的电子门禁系统使用采用MAC或数字签名等技术对记录进行完整性保护，保证进出数据记录的存储完整性。
3. 视频监控音像记录数据完整性：采用基于密码技术的的视频监控系统，视频监控系统的音像记录应严格进行完整性保护，完整的音像记录是实现安全管理、事后追责的重要基础。使用采用MAC或数字签名等技术对记录进行完整性保护，保证视频监控音像记录数据的存储完整性。

5.2.2 本系统密码应用技术方案-物理和环境

本项目对应方案如表5.1所示。

表 5.1 密码应用技术方案表-物理与环境

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品 | 方案描述 | 结论 |
| 机房AADDDW | 身份鉴别 | 国密电子门禁系统 | 物理和环境安全中的身份鉴别属于高风险项，指标要求采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。建议采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，保护物理访问控制身份鉴别信息。符合该标准的电子门禁系统使用SM4等算法进行密钥分散，实现门禁卡的一卡一密，并基于SM4等算法鉴别人员身份。但考虑到系统门禁系统现状和资金问题，也可使用缓解措施，也可采用此高风险项的缓解措施：采用基于生物识别技术（如指纹等）对进入人员进行身份鉴别；如指纹、人脸识别的门禁系统；采用基于普通电子门禁系统并配合人工登记和视频监控，保证重要区域进入人员身份的真实性。采用如上两种方式，属于此高风险项的缓解措施，可酌情降低风险等级。 | 符合 |
| 机房AADDDW | 电子门禁记录数据存储完整性 | 国密电子门禁系统 | 采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，电子门禁系统进出记录应严格进行完整性保护，完整的进出记录是实现安全管理、事后追责的重要基础。符合该标准的电子门禁系统使用采用MAC或数字签名等技术对记录进行完整性保护，保证进出数据记录的存储完整性。 | 符合 |
| 机房AADDDW | 视频监控记录数据存储完整性 | 国密视频监控 | 采用基于密码技术的的视频监控系统，视频监控系统的音像记录应严格进行完整性保护，完整的音像记录是实现安全管理、事后追责的重要基础。使用采用MAC或数字签名等技术对记录进行完整性保护，保证视频监控音像记录数据的存储完整性。 | 不符合 |

5.3 网络和通信

5.3.1 密码应用技术方案

系统应部署符合密码相关国家、行业标准要求的密码设备或产品，保证通信实体身份的真实性；保证通信过程中数据的完整性和机密性；保证网络边界访问控制信息的完整性；保证接入的设备身份真实性。

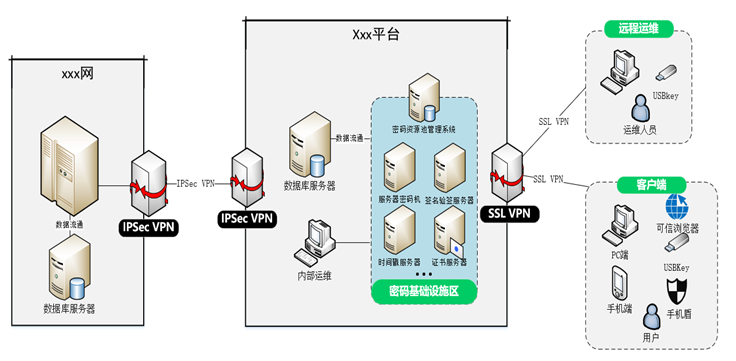


图 5.5 网络和通信安全架构图

1. 身份鉴别：客户端对服务端响应报文中数字证书进行解析，如未发现异常则保证通信实体的真实性。
2. 通信数据完整性和通信过程中重要数据的机密性：部署已通过商用密码机构认证的密码产品或者使用合规的国密算法实现对通信数据完整性保护和通信过程中重要数据的机密性保护。
3. 网络边界访问控制信息的完整性：部署已通过商用密码机构认证的

密码产品或者调用服务器密码机实现对网络边界访问控制信息的完整性保护。

1. 安全接入认证：通过网络安全设备控制外部设备接入，只有已授权的外部设备可以接入到内部网络，保证接入设备的身份真实性。

5.3.2 本系统密码应用技术方案-网络和通信

表5.2 密码应用技术方案表-网络和通信

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品 | 方案描述 | 结论 |
| 互联网运维人员与系统之间的通信信道 | 身份鉴别 | SSL VPN | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 互联网运维人员与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 互联网运维人员与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 互联网运维人员与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 互联网运维人员与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 互联网PC浏览器与系统之间的通信信道 | 身份鉴别 | SSL VPN | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 互联网PC浏览器与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 互联网PC浏览器与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 互联网PC浏览器与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 互联网PC浏览器与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 身份鉴别 | SSL VPN+定制开发+USBKey+签名验签服务器 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 互联网PC客户端与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 互联网PC客户端与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 移动端APP与系统之间的通信信道 | 身份鉴别 | SSL VPN | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 移动端APP与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 移动端APP与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 移动端APP与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 移动端APP与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 身份鉴别 | 定制开发+协同签名系统 | 空 | 空 |
| 互联网PC客户端与系统之间的通信信道 | 通信数据完整性 | 空 | 空 | 空 |
| 互联网PC客户端与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 空 | 空 |
| 互联网PC客户端与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 空 | 空 |
| 互联网PC客户端与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 办公内网运维人员与系统之间的通信信道 | 身份鉴别 | SSL VPN | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 办公内网运维人员与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 办公内网运维人员与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 办公内网运维人员与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 办公内网运维人员与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 办公内网PC浏览器与系统之间的通信信道 | 身份鉴别 | SSL VPN | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的SSL VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 办公内网PC浏览器与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 互联网PC客户端与系统之间的通信信道 | 身份鉴别 | 定制开发+USBKey+签名验签服务器 | 空 | 空 |
| 互联网PC客户端与系统之间的通信信道 | 通信数据完整性 | 空 | 空 | 符合 |
| 互联网PC客户端与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 空 | 符合 |
| 互联网PC客户端与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 空 | 空 |
| 互联网PC客户端与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 物联网设备与系统之间的通信信道 | 身份鉴别 | IPSec VPN盒子 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 物联网设备与系统之间的通信信道 | 通信数据完整性 | 空 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 物联网设备与系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 物联网设备与系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 物联网设备与系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |
| 系统与其他业务系统之间的通信信道 | 身份鉴别 | IPSec VPN + Https | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中通信实体的身份鉴别 | 符合 |
| 系统与其他业务系统之间的通信信道 | 通信数据完整性 | 空 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中数据的完整性 | 符合 |
| 系统与其他业务系统之间的通信信道 | 通信过程中重要数据的机密性 | 空 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中重要数据的机密性 | 符合 |
| 系统与其他业务系统之间的通信信道 | 网络边界访问控制信息的完整性 | 空 | 部署的IPSec VPN安全网关已通过商用密码机构认证，可保证通信过程中访问控制信息的完整性 | 符合 |
| 系统与其他业务系统之间的通信信道 | 安全接入认证 | 无 | 等保三级系统不做此要求 | 不适用 |

5.4 设备和计算

5.4.1 密码应用技术方案

在设备和计算安全中主要是指管理员在对业务系统进行运维时，需要对运维管理员身份鉴别，保障网络环境中主机系统以及存储资源以及其上所承载的应用程序等重要数据的机密性和完整性。架构图如图 5.6所示：

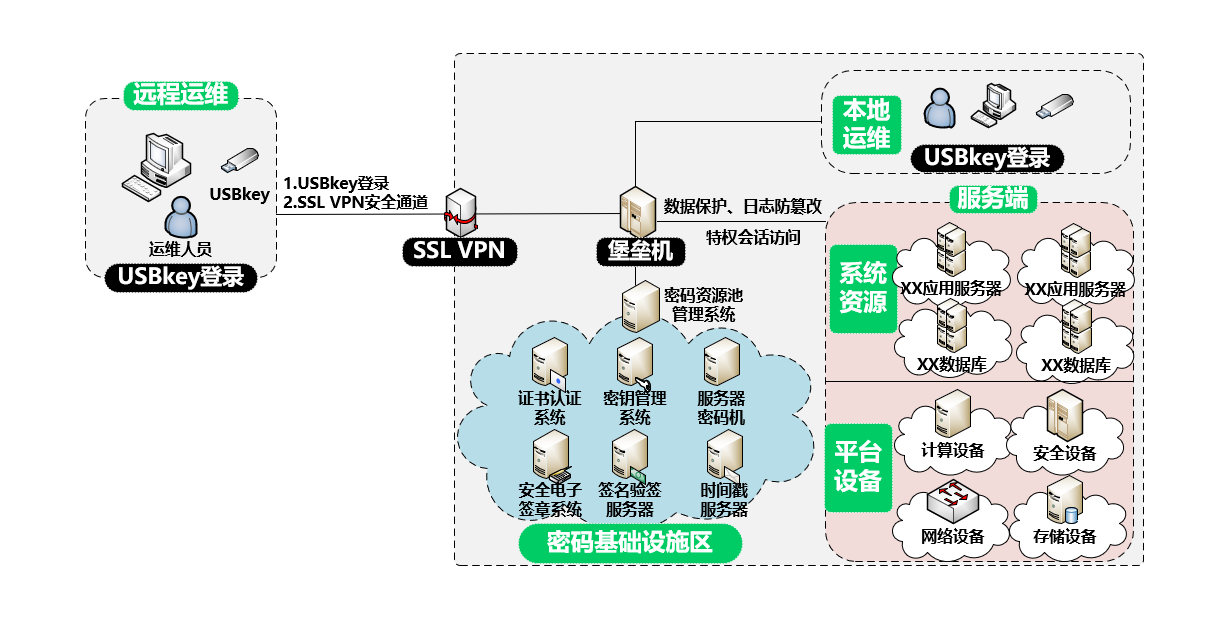


图 5.6 设备和计算安全架构图

1. **身份鉴别：**本系统由经批准的数字证书认证系统提供数字证书，在密码基础设施区部署堡垒机和签名验签服务器。运维人员配发USBKey（USBKey中存有数字证书），运维人员在PC端使用用户名+口令+USBKey的方式保证身份的真实性；登录堡垒机时验证运维人员的签名证书，通过后选择对应的应用服务器、数据库服务器等设备，通过SSH2协议对系统中的各业务应用服务器、各数据库服务器进行运维管理。以此实现对运维人员的安全身份鉴别，防止非授权人员登录。
2. **远程管理通道安全：**采用遵循密码相关国家标准和行业标准的VPN技术，使用密码产品SSL VPN安全网关登录堡垒机，再由堡垒机使用SSH2协议登录到各设备，以搭建安全的远程管理通道。
3. **系统资源访问控制信息完整性：**在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。
4. **重要信息资源安全标记完整性：**本系统不涉及重要信息的敏感标记。
5. **日志记录完整性：**在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC-SM3对应用服务器、数据库服务器等设备日志记录进行完整性保护。
6. **重要可执行程序完整性、重要可执行程序来源真实性：**在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。

5.4.2 本系统密码应用技术方案-设备和计算

表5.3 密码应用技术方案表-设备与计算

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品 | 方案描述 | 结论 |
| WWEQRW得到的 | 身份鉴别 | 无 | 运维人员在PC端使用用户名+口令+USBKey的方式登录到堡垒机，保证运维人员身份的真实性；通过堡垒机身份鉴别后，选择对应的设备，进行运维管理。不需要改造 | 符合 |
| WWEQRW得到的 | 远程管理通道安全 | SSL VPN+国密堡垒机 | 运维人员在通过具有商用产品证书的SSL VPN安全网关登录到国密堡垒机，进行设备的统一管理；国密堡垒机通过SSH2协议对系统中的各业务应用服务器、各数据库服务器和已通过商用密码产品认证的设备进行运维管理，建立安全的远程管理通道。 | 符合 |
| WWEQRW得到的 | 系统资源访问控制信息完整性 | 服务器密码机 | 对本系统涉及到的：1、Linux系统访问控制信息； 2、系统文件目录的访问控制信息； 3、Oracle/MySQL数据库中的数据访问控制信息； 4、堡垒机的权限访问控制信息；在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。（所涉及的Linux系统权限访问控制信息一般存储在incode结构体中，具体存储文件和路径需参考目标系统操作系统及其版本号；所涉及的Oracle数据库中的数据访问控制信息一般存储在CONTROL01.CTL/CONTROL02.CTL文件中，具体存储文件和路径需参考目标系统数据库及其版本号；所涉及的MySQL数据库中的数据访问控制信息，具体存储文件和路径需参考目标系统数据库及其版本号） | 符合 |
| WWEQRW得到的 | 重要信息资源安全标记完整性 | - | - | 不适用 |
| WWEQRW得到的 | 日志记录完整性 | 服务器密码机 | 在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC-SM3对应用服务器、数据库服务器等设备日志记录进行完整性保护 | 符合 |
| WWEQRW得到的 | 重要可执行程序完整性、重要可执行程序来源真实性 | 签名验签服务器 | 在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。 | 符合 |
| SSL VPN | 身份鉴别 | 证书认证系统、USBKey、签名验签服务器 | 本系统由经批准的证书认证系统提供数字证书，在密码基础设施区部署签名验签服务器。运维人员配发USBKey（USBKey中存有数字证书），运维人员在PC端使用用户名+口令+USBKey的方式保证身份的真实性；登录登陆管理系统时通过中间件调用签名验签服务器，验证运维人员的签名证书，通过后选择对应的应用服务器、数据库服务器等设备，通过SSH协议对系统中的各业务应用服务器、各数据库服务器进行运维管理。以此实现对运维人员的安全身份鉴别，防止非授权人员登录。 | 符合 |
| SSL VPN | 远程管理通道安全 | SSL VPN | 运维人员通过具有商用产品证书的SSL VPN安全网关接入内网，并通过SSH2协议登录到各业务应用服务器、各数据库服务器等通用服务器和已通过商用密码产品认证的设备，以建立安全的远程管理通道。 | 符合 |
| SSL VPN | 系统资源访问控制信息完整性 | 服务器密码机 | 对本系统涉及到的：1、Windows系统访问控制信息；2、系统文件目录的访问控制信息；3、Oracle/MySQL数据库中的数据访问控制信息；在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。（所涉及的Windows系统权限访问控制信息一般存储在本地计算机SAM文件中，路径一般为C:\Windows\System32\config，具体存储文件和路径需参考目标系统操作系统及其版本号；所涉及的SQL Server数据库中的数据访问控制信息，具体存储文件和路径需参考目标系统数据库及其版本号） | 符合 |
| SSL VPN | 重要信息资源安全标记完整性 | - | - | 不适用 |
| SSL VPN | 日志记录完整性 | 服务器密码机 | 在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC-SM3对应用服务器、数据库服务器等设备日志记录进行完整性保护 | 符合 |
| SSL VPN | 重要可执行程序完整性、重要可执行程序来源真实性 | 签名验签服务器 | 在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。 | 符合 |
| IPsec VPN | 身份鉴别 | 无 | 运维人员在PC端使用用户名+口令+USBKey的方式登录到堡垒机，保证运维人员身份的真实性；通过堡垒机身份鉴别后，选择对应的设备，进行运维管理。不需要改造 | 符合 |
| IPsec VPN | 远程管理通道安全 | SSL VPN+国密堡垒机 | 运维人员在通过具有商用产品证书的SSL VPN安全网关登录到国密堡垒机，进行设备的统一管理；国密堡垒机通过SSH2协议对系统中的各业务应用服务器、各数据库服务器和已通过商用密码产品认证的设备进行运维管理，建立安全的远程管理通道。 | 符合 |
| IPsec VPN | 系统资源访问控制信息完整性 | 服务器密码机 | 对本系统涉及到的：1、Linux系统访问控制信息； 2、系统文件目录的访问控制信息； 3、Oracle/MySQL数据库中的数据访问控制信息； 4、堡垒机的权限访问控制信息；在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。（所涉及的Linux系统权限访问控制信息一般存储在incode结构体中，具体存储文件和路径需参考目标系统操作系统及其版本号；所涉及的Oracle数据库中的数据访问控制信息一般存储在CONTROL01.CTL/CONTROL02.CTL文件中，具体存储文件和路径需参考目标系统数据库及其版本号；所涉及的MySQL数据库中的数据访问控制信息，具体存储文件和路径需参考目标系统数据库及其版本号） | 符合 |
| IPsec VPN | 重要信息资源安全标记完整性 | - | - | 不适用 |
| IPsec VPN | 日志记录完整性 | 服务器密码机 | 在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC-SM3对应用服务器、数据库服务器等设备日志记录进行完整性保护 | 符合 |
| IPsec VPN | 重要可执行程序完整性、重要可执行程序来源真实性 | 签名验签服务器 | 在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。 | 符合 |
| 堡垒机 | 身份鉴别 | 无 | 运维人员在PC端使用用户名+口令+USBKey的方式登录到堡垒机，保证运维人员身份的真实性；通过堡垒机身份鉴别后，选择对应的设备，进行运维管理。不需要改造 | 符合 |
| 堡垒机 | 远程管理通道安全 | SSL VPN+国密堡垒机 | 运维人员在通过具有商用产品证书的SSL VPN安全网关登录到国密堡垒机，进行设备的统一管理；国密堡垒机通过SSH2协议对系统中的各业务应用服务器、各数据库服务器和已通过商用密码产品认证的设备进行运维管理，建立安全的远程管理通道。 | 符合 |
| 堡垒机 | 系统资源访问控制信息完整性 | 服务器密码机 | 对本系统涉及到的：1、Linux系统访问控制信息； 2、系统文件目录的访问控制信息； 3、Oracle/MySQL数据库中的数据访问控制信息； 4、堡垒机的权限访问控制信息；在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。（所涉及的Linux系统权限访问控制信息一般存储在incode结构体中，具体存储文件和路径需参考目标系统操作系统及其版本号；所涉及的Oracle数据库中的数据访问控制信息一般存储在CONTROL01.CTL/CONTROL02.CTL文件中，具体存储文件和路径需参考目标系统数据库及其版本号；所涉及的MySQL数据库中的数据访问控制信息，具体存储文件和路径需参考目标系统数据库及其版本号） | 符合 |
| 堡垒机 | 重要信息资源安全标记完整性 | - | - | 不适用 |
| 堡垒机 | 日志记录完整性 | 服务器密码机 | 在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC-SM3对应用服务器、数据库服务器等设备日志记录进行完整性保护 | 符合 |
| 堡垒机 | 重要可执行程序完整性、重要可执行程序来源真实性 | 签名验签服务器 | 在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。 | 符合 |

5.5 应用和数据

5.5.1 密码应用技术方案

针对在应用和数据安全层面的密码应用需求，本节提出对应的功能设计，主要包括身份鉴别、访问控制信息完整性、重要数据传输完整性、重要数据传输机密性、重要数据存储机密性、重要数据存储完整性、不可否认性，应用和数据安全架构图如图 5.7所示。

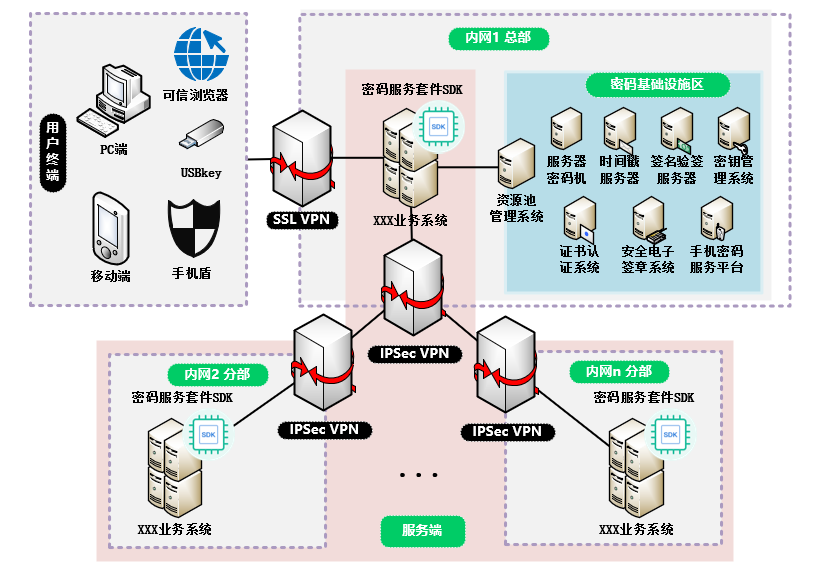


图 5.7 应用和数据安全架构图

1. **身份鉴别：**在密码基础设施区部署符合密码相关国家、行业标准要求的签名验签服务器、USBKey，实现对登录用户的安全身份鉴别，保证应用系统用户身份的真实性，防止非授权人员登录。
2. **访问控制信息完整性：**在密码基础设施区部署服务器密码机，使用HMAC对系统应用的访问控制信息进行完整性保护，防止访问控制信息被篡改。
3. **重要信息资源安全标记完整性：**无（根据系统定义的安全标记进行有针对性的防护）
4. **重要数据传输机密性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2及SM3算法进行会话密钥交互，采用SM4算法对传输的数据信息进行机密性保护，防止其被非授权窃取。
5. **重要数据存储机密性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用SM4算法对数据信息存储进行机密性保护，防止其被非授权窃取。
6. **重要数据传输完整性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2算法进行会话密钥交互，采用HMAC算法对传输的数据信息进行完整性保护，防止其被非授权篡改。
7. **重要数据存储完整性：**在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用HMAC对数据信息存储进行完整性保护，防止其被非授权篡改。
8. **不可否认性：**在基础设施区部署时间戳服务器，在系统中重要数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性。

5.5.2 本系统密码应用技术方案-应用和数据

本项目对应方案如表5.4所示。

表5.4 密码应用技术方案表-应用和数据

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 测评对象 | 指标点 | 解决方案 | | |
| 密码产品 | 方案描述 | 结论 |
| 业务A | 身份鉴别 |  | 需双向认证的用户（如系统管理员）通过PC端登录业务系统时，使用账号+密码配合智能密码钥匙登录系统，智能密码钥匙采用数字证书方式认证，并在密码基础设施区部署签名验签服务器，提供对证书的验证。用户通过用户名+短信验证码登录，实现登录应用用户的身份鉴别，防止非授权人员登录。 | 不符合 |
| 业务A | 访问控制信息完整性 | 国密安全密码应用中间件、服务器密码机 | 在密码基础设施区部署服务器密码机和国密安全密码应用中间件，使用HMAC算法对系统应用的用户角色分配表、系统权限分配表、数据库权限分配表等访问控制信息进行完整性保护，防止访问控制信息被篡改。 | 符合 |
| 业务A | 重要信息资源安全标记完整性 | 无 | - | 不适用 |
| 业务A | 重要数据传输机密性 | 国密安全密码应用中间件、服务器密码机 | 客户端与服务端进行通信时，应用系统通过国密安全密码应用中间件数据加解密接口调用服务器密码机，采用SM2算法进行会话密钥交互，使用会话密钥采用SM4算法加密。服务端与服务端进行通信时，应用系统通过国密安全密码应用中间件数据加解密接口调用服务器密码机，采用基于ECC密码算法的数字信封功能，先使用对称密钥加密数据，再使用接收方公钥对对称密钥加密。 | 符合 |
| 业务A | 重要数据存储机密性 | 无 | 根据调研情况系统已经采用合规的密码算法对重要数据存储进行机密性保护，无需进行改造。 | 符合 |
| 业务A | 重要数据传输完整性 | 国密安全密码应用中间件、服务器密码机 | 在密码基础设施区部署服务器密码机，并在应用服务器上部署国密安全密码应用中间件，采用SM2算法进行会话密钥交互，使用会话密钥采用HMAC-SM3算法在数据传输前对数据进行完整性保护，防止其被非授权篡改。 | 符合 |
| 业务A | 重要数据存储完整性 | 无 | 根据调研情况系统已经采用合规的密码算法对重要数据存储进行机密性保护，无需进行改造。 | 符合 |
| 业务A | 不可否认性 | 无 | 本方案对不可否认性不适用。 | 不适用 |

5.6 密钥管理

5.6.1 密码应用技术方案

密码服务中，对称密钥全生命周期包括密钥的生成、存储、分发等，具体如表5.5所示。

5.6.2 本系统密码应用技术方案-密钥管理

表5.5 对称密钥全生命周期表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 密钥 | 生成 | 存储 | 分发 | 导入  导出 | 使用 | 备份  恢复 | 归档 | 销毁 |
| 服务器密码机主密钥 | 由密钥管理员基于双人控制明文输入 | 服务器密码机内部存储 | 不涉及 | 通过专用介质导入导出，用于备份和恢复 | 服务器密码机内部使用 | 专用密钥存储介质存储分量 | 两个密钥分量单独由负责人保存 | 服务器密码机内部完成销毁 |
| 服务器密码机关键数据加解密密钥 | 服务器密码机内部生成 | 服务器密码机主密钥加密存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部完成备份和恢复 | 服务器密码机内部完成归档 | 服务器密码机内部完成销毁 |
| 服务器密码机镜像密钥 | 服务器密码机内部生成 | 服务器密码机主密钥加密存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部完成备份和恢复 | 服务器密码机内部完成归档 | 服务器密码机内部完成销毁 |
| 服务器密码机日志密钥 | 服务器密码机内部生成 | 服务器密码机主密钥加密存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 服务器密码机内部完成备份和恢复 | 服务器密码机内部完成归档 | 服务器密码机内部完成销毁 |
| 应用主密钥 | 虚拟密码机内部生成 | 虚拟密码机内部存储 | 通过租户证书、设备证书，租户和设备建立安全信道实现分发 | 通过安全信道加密导入导出 | 虚拟密码  机内部使用 | 通过租户证书、设备证书，租户和设备建立安全信道实现备份和恢复 | 租户指定在一台虚拟密码机内部归档 | 虚拟密码机内部完成销毁 |

密码服务中，非对称密钥全生命周期包括密钥的生成、存储、分发等，具体如表5.6所示：

表5.6 非对称密钥全生命周期表

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 密钥 | 生成 | 存储 | 分发 | 导入  导出 | 使用 | 备份  恢复 | 归档 | 销毁 |
| 服务器密码机非对称私钥 | 服务器密码机内部生成 | 服务器密码机内部存储 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 不涉及 | 不涉及 | 服务器密码机内部完成销毁 |
| 服务器密码机非对称公钥 | 服务器密码机内部生成 | 以公钥形式存储 | 以数字证书形式分发 | 以公钥证书形式导入导出 | 虚拟密码机迁移时使用 | 不涉及 | 不涉及 | CA证书平台进行撤销 |
| 用户非对称私钥 | 智能密钥钥匙生成 | 智能密钥钥匙内部存储 | 不涉及 | 不涉及 | 智能密钥钥匙内部使用 | 不涉及 | 不涉及 | 智能密钥钥匙内部完成销毁 |
| 用户非对称公钥 | 智能密钥钥匙生成 | 以公钥形式存储 | 以数字证书形式分发 | 以公钥证书形式导入导出 | 业务应用使用 | 不涉及 | 不涉及 | CA证书平台进行撤销 |

5.7 密码应用部署

密码应用部署拓扑图如图所示：

1. 客户端在PC端配发USBKey智能密码钥匙。授权用户通过PC端登录，采用SM2数字证书认证机制，使用USBKey，与安全通道中的SSL VPN综合安全网关之间，实现双向身份认证，确保授权用户身份的真实性。

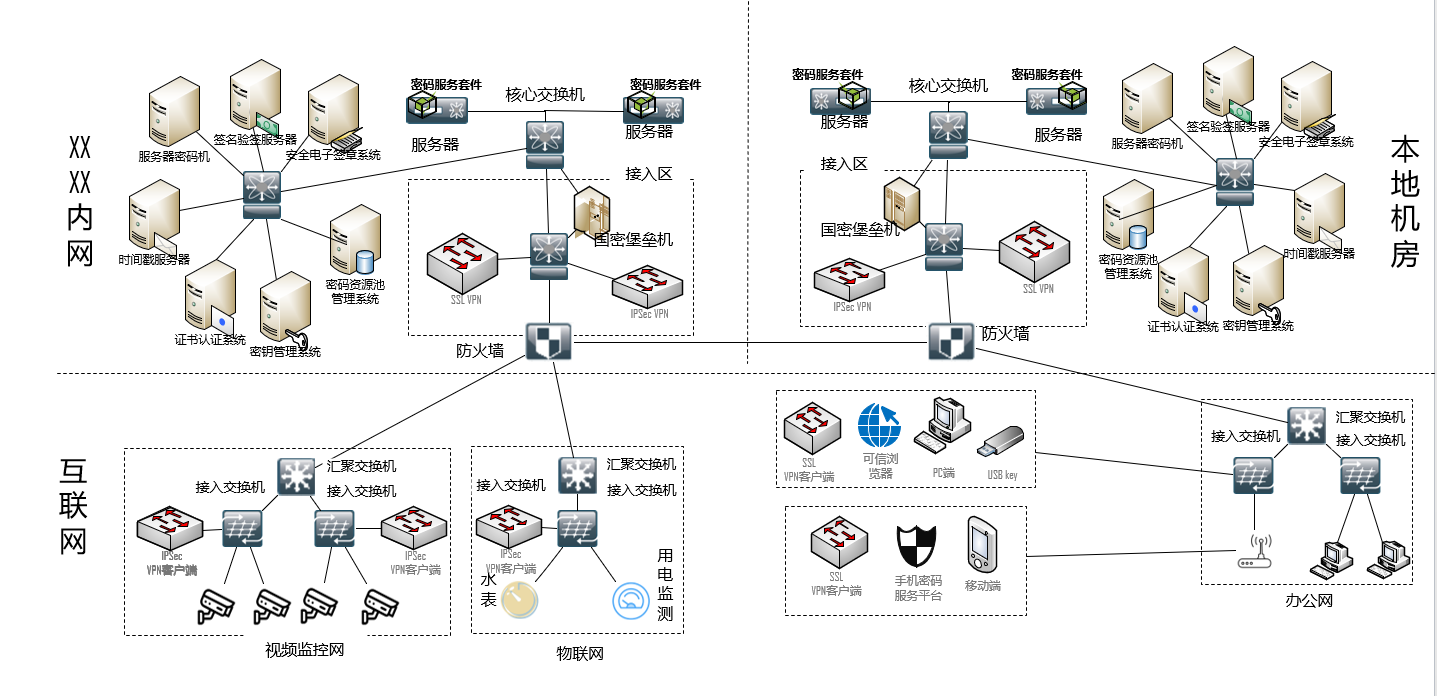


图 5.8 密码应用部署拓扑图

1. 安全通道部署SSL VPN综合安全网关，系统运维人员配发智能密码钥匙，由CA机构签发SM2数字证书，实现客户端与SSL VPN综合安全网关之间的双向身份认证。运维人员通过安装SSL VPN客户端实现安全接入。
2. 服务端包括交换机以及密码基础设施区，密码基础设施包括服务器密码机、签名验签服务器、时间戳服务器、数字证书认证系统、国密安全密码应用中间件为上层提供各种密码服务：服务器密码机可以提供加解密服务和密钥管理服务；签名验签服务器可以提供签名验签服务，实现身份验证；时间戳服务器的时间戳签发服务可以为操作节点签发时间戳，实现操作行为可追溯；证书认证系统为用户的身份鉴别提供真实性服务；国密安全密码应用中间件可以提供重要数据存储的机密性与完整性保护。

5.8 密码软硬件产品

5.8.1 密码软硬件产品清单

通过上述分析，该目标系统的密码应用改造所需的密码产品所包括硬件、软件以及相关的服务，如表5.7所示。

表5.7 密码软硬件产品清单表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 部署位置 | 主要用途 | 数量  (台/套) | 备注 |
| 1 | 服务器密码机 | 密码基础设施区 | 用途 | 2 | 一主一备，可按需动态扩展 |
| 2 | 签名验签服务器 | 密码基础设施区 | 用途 | 2 | 一主一备，可按需动态扩展 |
| 3 | 国密安全密码应用中间件 | - | 用途 | 1 |  |
| 4 | 国密数字证书 | - | 用途 | 按需 |  |
| 5 | 智能密码钥匙 | - | 用途 | 按需 |  |
| 6 | SSL VPN安全网关 | 网络接入区 | 用途 | 1 | 一主一备，可按需动态扩展 |
| 7 | 密码应用技术服务 | 密码基础设施区 | 用途 | 1 |  |

5.8.2 密码软硬件产品介绍

* 1. **服务器密码机：**服务器密码机为整个系统提供基本的密码运算服务以及基础密钥管理服务。遵循GM/T 0030《服务器密码机技术规范》及GM/T 0059《服务器密码机检测规范》；具有商用密码产品认证证书；支持SM2、SM3、SM4等国产密码算法；支持RSA、3DES、AES、SHA等常见国际算法；支持至少三层密钥结构，支持管理密钥、用户密钥、设备密钥、密钥加密密钥、会话密钥的管理；支持对称与非对称密钥的生成及管理。采用两路独立由国家密码管理局批准使用的物理噪声源产生器芯片生成的真随机数；设备内可存储至少100个对称密钥以及32对非对称密钥，并且支持加密存储或微电保护存储；支持数据加密/解密、签名/验签、杂凑算法等类型的密码运算；分别赋予不同的操作权限，并采用数字签名技术，实现对登录用户的强身份认证；支持SDF、JEC、P11接口。
  2. **密钥管理系统：**为用户或应用系统生产、分发和管理密钥的系统及设备，持对称密钥和非对称密钥的全生命周期管理，实现密钥的生成、存储、保护、恢复、分配、注册、注销和归档，以及密钥管理的审计和跟踪、密钥管理系统的访问控制等功能；支持SM2、SM4等国产密码算法，支持RSA、DES、3DES、AES常见国际算法。遵循GM/T 0034《基于SM2密码算法的证书认证系统密码及其相关安全技术规范》、GM/T 0051《密码设备管理对称密钥管理技术规范》。
  3. **国密安全密码应用中间件**：国密安全密码应用中间件用于保证数据存储的安全。支持SM1、SM2、SM3、SM4等国产密码算法；以数据加密密钥管理服务端与数据加密套件（SDK）的形式向业务应用系统提供数据加解密服务，屏蔽不同型号服务器密码机的异构性，对服务器密码机资源进行基本的资源调度。

数据加密服务：

国密安全密码应用中间件由数据加密插件和服务器密码机组成，如图 5.3所示，明文可以通过数据插件套件进行数据加密并由服务器密码机进行存储保存。

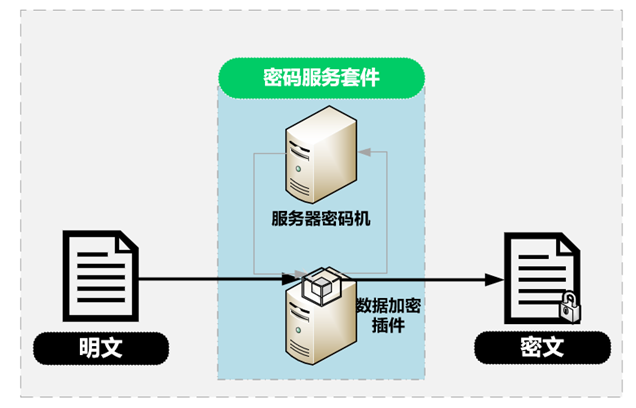


图 5.3 国密安全密码应用中间件设备图

① 数据加密插件

数据加密插件面向应用提供透明的加解密功能，插件与数据加密管理平台进行交互，获取加解密策略以及密钥，并提供数据库操作数据。通过数据加密插件，应用无需再进行任何额外的改造，即可向数据库传输密文，数据以密文的形式存储于数据库中。

数据加密支持结构化和非结构化的数据。

②签名验签服务功能

签名验签服务套件以软件形式部署于密钥管理服务平台中，签名验签服务，提供数字签名、签名验证服务，用来保障重要业务数据、权限管理数据、日志数据的完整性。签名验签服务：

签名验签服务套件对外的主要服务接口包括：

* 初始化接口：设置服务器连接、验证服务的访问权限；
* 数据签名接口：为应用系统提供数据签名接口；
* 签名验证接口：为应用系统提供签名数据的验证接口，并将签名数字证书信息解析返回给应用系统。

③完整性保护服务功能

完整性保护服务套件面向重要数据的完整性保护需求，结合数字证书、签名验签、服务器密码机提供完整性保护服务，提供基于消息鉴别码的完整性保护（HMAC-SM3）算法和基于数字签名的完整性保护（SM2-SM3）算法，支持数据完整性保护、文件完整性保护服务等。主要功能：

* 访问控制信息完整性
* 重要程序或文件完整性保护
* 日志记录完整性
  1. **安全电子签章系统：**电子签章将传统印章与电子签名技术进行结合，通过采用密码、图像处理等技术，使电子签名操作和纸质文件盖章操作具有相同的可视效果。提供电子印章管理、电子签章/验章等功能的密码应用系统。电子签章基于公钥密码技术标准体系，以电子形式对电子文档进行数字签名及签章，以确保文档来源的真实性以及文档的完整性，防止对文档未经授权的篡改，并确保签章行为的不可否认性。遵循GM/T 0031《安全电子签章密码技术规范》。支持SM2、SM3国产密码算法。具有商用密码产品认证证书
  2. **数字证书认证系统：**数字证书作用是为用户提供数字证书的申请、审核、签发、注销、更新、查询、下载等全生命周期的综合管理功能。符合国家标准GB/T 25056-2018《信息安全技术 证书认证系统密码及相关安全技术规范》；支持SM2、SM3、SM4等国产密码算法；且具有商用密码产品认证证书。
  3. **手机密码服务平台：**手机密码服务平台为移动互联网、移动设备提供密码运算支撑，用于身份认证、电子签名、数据保护等密码服务。支持基于数字证书的身份鉴别。提供用户个人敏感信息保护。提供移动端密钥生成、分发、使用、存储、销毁等全生命周期管理。提供数据签名服务接口，支持从业务系统发起签名请求，服务器与用户手机端共同完成协同签名操作流程。支持SM2、SM3、SM4商密算法以及RSA、DES、AES、SHA等国际密码算法。
  4. **签名验签服务器：**对各种类型的电子数据给出基于数字证书的数字签名服务,并向签名数据验证其签名的真实性与有效性的专用服务器。数字签名验证服务器可普遍应用在网上审批、银行、办公、支付与证券等电子政务、商务与企业信息化中向业务系统给出安全保护。

具有身份认证功能、数据签名功能、验证签名功能、系统备份功能、日志管理功能等特点。

5.9 安全与合规性分析

5.9.1 物理和环境

物理与环境安全与合规性分析结果如表5.8所示：

表5.8 安全与合规性分析表-物理和环境

|  |  |  |  |
| --- | --- | --- | --- |
| **指标点** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合/不适用）** |
| 身份鉴别 | 机房AADDDW | 符合 | 符合 |
| 电子门禁记录数据存储完整性 | 机房AADDDW | 符合 | 符合 |
| 视频监控记录数据存储完整性 | 机房AADDDW | 符合 | 符合 |

5.9.2 网络和通信

表5.9 安全与合规性分析表-网络和通信

|  |  |  |  |
| --- | --- | --- | --- |
| **指标点** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合，缓解/不符合/不适用）** |
| 身份鉴别 | 互联网运维人员与系统之间的通信信道 | 符合 | 符合 |
|  | 互联网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 符合 |  |
|  | 移动端APP与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 办公内网运维人员与系统之间的通信信道 | 符合 |  |
|  | 办公内网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 物联网设备与系统之间的通信信道 | 符合 |  |
|  | 系统与其他业务系统之间的通信信道 | 符合 |  |
| 通信数据完整性 | 互联网运维人员与系统之间的通信信道 | 符合 | 符合 |
|  | 互联网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 符合 |  |
|  | 移动端APP与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 办公内网运维人员与系统之间的通信信道 | 符合 |  |
|  | 办公内网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 物联网设备与系统之间的通信信道 | 符合 |  |
|  | 系统与其他业务系统之间的通信信道 | 符合 |  |
| 通信过程中重要数据的机密性 | 互联网运维人员与系统之间的通信信道 | 符合 | 符合 |
|  | 互联网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 符合 |  |
|  | 移动端APP与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 办公内网运维人员与系统之间的通信信道 | 符合 |  |
|  | 办公内网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 物联网设备与系统之间的通信信道 | 符合 |  |
|  | 系统与其他业务系统之间的通信信道 | 符合 |  |
| 网络边界访问控制信息的完整性 | 互联网运维人员与系统之间的通信信道 | 符合 | 符合 |
|  | 互联网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 符合 |  |
|  | 移动端APP与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 办公内网运维人员与系统之间的通信信道 | 符合 |  |
|  | 办公内网PC浏览器与系统之间的通信信道 | 符合 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 空 |  |
|  | 物联网设备与系统之间的通信信道 | 符合 |  |
|  | 系统与其他业务系统之间的通信信道 | 符合 |  |
| 安全接入认证 | 互联网运维人员与系统之间的通信信道 | 不适用 | 不适用 |
|  | 互联网PC浏览器与系统之间的通信信道 | 不适用 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 不适用 |  |
|  | 移动端APP与系统之间的通信信道 | 不适用 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 不适用 |  |
|  | 办公内网运维人员与系统之间的通信信道 | 不适用 |  |
|  | 办公内网PC浏览器与系统之间的通信信道 | 不适用 |  |
|  | 互联网PC客户端与系统之间的通信信道 | 不适用 |  |
|  | 物联网设备与系统之间的通信信道 | 不适用 |  |
|  | 系统与其他业务系统之间的通信信道 | 不适用 |  |

5.9.3 设备和计算

表5.10 安全与合规性分析表-设备和计算

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合，缓解/不符合/不适用）** |
| 身份鉴别 | WWEQRW得到的 | 符合 | 符合 |
|  | SSL VPN | 符合 |  |
|  | IPsec VPN | 符合 |  |
|  | 堡垒机 | 符合 |  |
| 远程管理通道安全 | WWEQRW得到的 | 符合 | 符合 |
|  | SSL VPN | 部分符合 |  |
|  | IPsec VPN | 符合 |  |
|  | 堡垒机 | 符合 |  |
| 系统资源访问控制信息完整性 | WWEQRW得到的 | 符合 | 符合 |
|  | SSL VPN | 符合 |  |
|  | IPsec VPN | 符合 |  |
|  | 堡垒机 | 符合 |  |
| 重要信息资源安全标记完整性 | WWEQRW得到的 | 不适用 | 不适用 |
|  | SSL VPN | 不适用 |  |
|  | IPsec VPN | 不适用 |  |
|  | 堡垒机 | 不适用 |  |
| 日志记录完整性 | WWEQRW得到的 | 符合 | 符合 |
|  | SSL VPN | 符合 |  |
|  | IPsec VPN | 符合 |  |
|  | 堡垒机 | 符合 |  |
| 重要可执行程序完整性、重要可执行程序来源真实性 | WWEQRW得到的 | 符合 | 符合 |
|  | SSL VPN | 符合 |  |
|  | IPsec VPN | 符合 |  |
|  | 堡垒机 | 符合 |  |

5.9.4 应用和数据

表5.11 安全与合规性分析表-应用和数据

|  |  |  |  |
| --- | --- | --- | --- |
| **测评单元** | **测评对象** | **测评指标符合情况（符合/部分符合/不符合，缓解/不符合/不适用）** | **单元测评结果（符合/部分符合/不符合，缓解/不符合/不适用）** |
| 身份鉴别 | 业务A | 数据查询出错 | 数据查询出错 |
| 访问控制信息完整性 | 业务A | 符合 | 符合 |
| 重要信息资源安全标记完整性 | 业务A | 不适用 | 不适用 |
| 重要数据传输机密性 | 业务A | 符合 | 符合 |
| 重要数据存储机密性 | 业务A | 符合 | 符合 |
| 重要数据传输完整性 | 业务A | 符合 | 符合 |
| 重要数据存储完整性 | 业务A | 符合 | 符合 |
| 不可否认性 | 业务A | 不适用 | 不适用 |

6 密码安全管理方案

保障商用密码应用的合规性、正确性和有效性，不能仅靠技术，配套的管理也是必不可少的。根据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，分别从管理制度、管理机构、建设运行、密钥管理、密码软硬件管理、人员管理和应急处置等几方面提出密码安全管理方案，建立配套密码安全管理制度，保障信息系统的正常运行以及数据安全，指导、规范信息系统密码应用的规划、建设、运行、应急及测评，为该系统提供管理方面的密码应用安全保障。

6.1 管理制度

依据《基本要求》《商用密码应用安全性评估管理办法（试行）》《信息系统密码测评要求（试行）》《商用密码应用安全性评估测评过程指南（试行）》《商用密码应用安全性评估测评作业指导书（试行）》等标准规范及管理要求为基础，结合ISO 270001(GB/T 22080)的体系的PDCA过程和ISO 27002（GB/T 22081）的14个控制域规范，同时兼顾监管部门的相关安全规范，整合企业自身的IT服务管理体系和技术安全控制体系，通过体系规范化、管理流程化、测量指标化、操作工具化等方式来确保管理体系设计的落地。密码安全管理制度体系主要包括：密码管理机构、密码建设、密钥管理、人员、设备等密码管理相关内容。此外同步在单位现有的制度发布流程中补充密码相关管理制度发布流程，待新制定的密码安全管理制度和操作规范内部评审通过后，按照密码相关管理制度发布流程予以发布并遵照执行。

本管理办法适用于本单位密码设备、密钥、相关信息系统的管理、操作和维护活动。

本管理办法所称密码设备，包括但不限于服务器密码机签名验签服务器、数字证书认证系统、智能密码钥匙等。

本管理办法所称密钥，包括但不限于非对称密钥对、对称密钥、MAC密钥等。

管理办法的执行机构是测试项目A。

6.2 管理机构

1. 本单位设立“测试项目A密码管理组织”，全面负责密钥生命周期、密码设备、设备证书的管理工作。
2. 测试项目A专网密码管理组织至少由一名密码管理负责人、两名安全审计员、一名密码设备管理员、两名密钥操作员、一名密钥保管员、一名档案管理员组成。
3. 所有的审批和操作指定专人负责，各类人员均应明确工作职责和管理权限，未经相关领导批准，不得擅自互换或代替。密码设备的管理账号、口令卡不得多人共用。
4. 密码管理负责人全面负责本单位密码管理的各项工作，统筹密码相关人员及工作安排，组织密码安全管理制度的制定及发布，负责密码相关人员考核等，组织开展定期或不定期的专项辅导检查工作。
5. 安全审计员负责监督审计本单位密码安全管理的各项工作，及时制止不正确操作，杜绝违规操作或越权操作行为。严格监督本单位密码相关重要岗位的工作状况，对不适合密码管理与维护工作或发现有不良行为的人员，提出调整建议。协助完成定期或不定期的专项辅导检查工作。
6. 密码设备管理员可由机房系统管理员兼任，负责维护密码设备正常运行，履行机房安全管理工作的一般性要求。协助完成定期或不定期的专项辅导检查工作。
7. 密钥操作员负责密钥的具体操作，完成密钥生成、备份、恢复、删除等操作过程。协助完成定期或不定期的专项辅导检查工作。
8. 密钥保管员负责密钥保管工作。接收密钥资料（组件），验证接收到的密钥资料是否受损；在监督下销毁密钥组件备份介质。协助完成定期或不定期的专项辅导检查工作。
9. 档案管理员负责收集、归档所有的审批和登记表格等密钥档案，按不同的操作特征和类型分类，保存在档案室、磁带备份室等安全区域；对档案建立较高的保密级别，未经书面授权，不允许借阅、复制及传播。维护经管理人 员授权后使用密钥的记录。协助完成定期或不定期的专项辅导检查工作。
10. 各类密码相关管理人员任用前，需签订保密协议，对本单位的密码设备配置、密钥、登录口令、敏感工作内容等均有保密义务。
11. 各类密码相关管理人员上岗前，需要参与必要的培训，包括熟悉密码相关管理制度，掌握各种密码设备的操作方法，明确相关工作流程规范等。
12. 各类密码相关管理人员每年应接受单位的考核，考核优秀者将给予奖励，考核不达标者要求重新参加培训，考核严重不合格者将调离本岗位。
13. 各类密码相关管理人员离职、退休或换岗前，需交回其管理的相关管理员介质、备份介质等密钥相关载体，密码管理负责人任命新任管理员后，把这些载体重新分配给新任管理员保管。新任密钥管理员上岗后，应及时召集其他密码管理员修改含有系统密钥的密码设备密码。

6.3 建设运行

系统的建设运行过程中，应注意的以下8点：

1. 测试项目A建设的信息系统，需要使用密码产品或密码模块时，应优先采购具有国家密码管理部门颁发的密码产品型号证书的密码产品或密码模块，若不能选购有资质密码产品，需要提供合理说明。
2. 测试项目A建设的信息系统，当需要使用密码服务时，应优先采购具有电子认证服务许可的电子认证机构的服务。
3. 测试项目A建设的信息系统，当需要使用密码算法时，应优先选择国家密码管理部门批准的密码算法，若不能采用国家密码管理部门批准的密码算法，需要提供合理说明。
4. 系统在规划阶段，应制定密码应用建设方案，并组织专家对建设方案进行评审，若系统已投入运行，需在系统改造前制定密码应用建设方案，组织专家对建设方案进行评审。
5. 系统在建设阶段，应制定密码应用实施方案，若系统已投入运行，需在系统改造过程中制定密码应用实施方案。
6. 信息系统投入运行前，应经商用密码应用安全性测评机构进行安全性评估，评估通过后方可投入正式运行，若系统已投入运行，改造后的系统应进行商用密码应用安全性评估。
7. 信息系统投入运行后，每年应委托商用密码应用安全性测评机构开展密码应用安全性评估，若系统已投入运行，改造后的系统应每年进行商用密码应用安全性评估。
8. 制定应急预案，定期开展应急演练，形成完善的安全事件处理和上报机制。

6.4 密钥管理

密钥管理主要分为7个步骤，具体如下：

1. 密钥的操作需由密钥应用方提出申请，由密码管理负责人签字确认，并制定密钥操作执行人，在密码设备管理员准备好硬件环境后，由密钥执行人进行操作。
2. 密码设备初始化由密码管理负责人和密钥操作员执行操作。具有口令卡的密码设备，管理员卡由密码管理负责人和密钥操作员分别持有。
3. 密钥的生成由密钥操作员执行操作。密钥在密码设备内由密码模块随机产生，密钥（除公钥外）不可以明文方式出现在密码模块之外。服务器密码机密钥生成后应马上进行密钥的备份操作。
4. 密钥的备份由密钥操作员执行操作，产生的备份卡、备份数据等由密钥保管员保管。
5. 密钥的恢复由密钥操作员执行操作，从密钥保管员处获取备份介质和数据。
6. 密钥的销毁应先进行密钥删除操作，再由密钥保管员对密钥备份卡、密钥备份文件进行物理销毁。
7. 上述各类密钥操作过程均应由安全审计员登记并保存记录。

6.5 密码软硬件管理

1. 密码设备应放置在严格安全管理措施的机房内，安装在带锁机柜中，机柜背板固定安装，对于密码设备的操作，配备摄像监控进行全过程监控，严禁打开密码设备机壳。
2. 在应用系统中禁止非法连接密码设备，新购买的密码设备应修改缺省口令，在密码设备报废时，应删除存储在该设备中的密钥。
3. 密码设备维修与升级要根据需求提出书面申请；密码设备生产厂商、维护商专人持有效身份证明文件，经证实获准。档案管理员详细记录工作日志，包括设备类型、故障现象、维修时间等要素。

6.6 人员管理

根据《基本要求》中密码安全管理人员方面的要求，测试项目A应制定相关的密码安全管理人员管理制度：

1. 设置内部密码专题培训机制，每6个月组织一次，由内部人员或聘请外部专家担任培训讲师，内容涉及密码相关法律法规和标准规范、商用密码应用、商用密码应用安全性评估等多个方面，使相关人员了解密码相关的法律和法规，掌握密码基本原理，并遵照执行。
2. 在密码应用系统建设完成后，安排项目建设单位、相关密码设备厂商对本系统部署使用的所有密码产品进行操作培训，确保相关人员能够正确配置使用本系统中部署的密码产品。
3. 结合测试项目A情况，分别设立密钥管理员、安全审计员、密码操作员等岗位，明确各岗位职责，对关键岗位建立多人共管机制，每个岗位均由2人担任；设备与系统的管理和使用账号不得多人共用。
4. 在现有的安全管理制度中，补充密码相关人员考核、奖惩、保密、调离制度，每年对密钥管理人员、安全审计人员、密码操作人员组织一次考核，对考核成绩优异的予以表扬和奖励，考核成绩不合格者，进行批评教育；密钥管理人员、安全审计人员、密码操作人员与单位订保密协议，承担保密义务，相关人员若要调离岗位时，按照制定的人员调离制度承担相应的保密义务。

6.7 应急方案

根据《基本要求》中安全管理应急方面的要求，测试项目A应制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施。主要包括：

1. 对信息系统现有的应急管理制度进行完善，补充制定密码相关应急处置预案，并做好应急资源准备，明确密码安全事件处理流程及其它管理措施。
2. 当信息系统发生密码相关安全事件时，在事发后/事件处置完成后及时向用户主管单位进行报告。

6.7.1 潜在的安全事件分析

1. 事件分类

按项目时间周期划分，对系统可用性、安全性会造成影响的密码应用安全事件可以归纳为如下两类。

* 1. 项目实施过程中的安全事件

① 业务系统密码应用集成故障：因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统无法正常使用密码产品的事件。

② 密码产品部署故障：因密码产品实施人员工作疏忽，造成密码产品无法正常工作的事件。

③ 业务系统密码应用集成漏洞：因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统密码应用存在漏洞的事件。典型的有：身份鉴别时对证书有效性验证不严谨，造成已过期的、被注销的、非受信CA颁发的证书可以通过认证；身份鉴别时没有采用随机数签名，造成身份鉴别信息可被重放攻击等。

* 1. 密码运行过程中出现的安全事件

① **系统管理员证书失效：**系统管理员证书在过期前没有及时去续期、系统管理员证书介质PIN锁死或介质损坏的事件。这些会造成系统管理员无法正常登录业务系统进行维护和管理工作，对业务系统的可用性可能会造成影响。

② **业务系统服务器证书失效：**业务系统的服务器证书在过期前没有及时去续期、业务系统IP或域名修改的事件。这些会造成服务器证书验证失败，影响业务系统的正常访问。

③ **服务端密钥泄露：**主要是指服务端的服务器密码机、签名验签服务器设备里的密钥（包括私钥、对称密钥、MAC密钥）泄露事件。这些会造成关键敏感数据存储与传输的私密性、完整性被破解。

④ **服务端密码设备故障：**主要是指服务端的服务器密码机、签名验签服务器设备故障事件。这些会造成业务系统身份鉴别、数据安全存储、数据安全传输等功能异常。

⑤ **密码设备的安全漏洞：**主要是指服务器密码机、签名验签服务器、智能密码钥匙等密码设备存在软件或硬件上的安全漏洞事件。这些可能会造成密码设备可以被非法访问、私钥可被猜测等安全问题。

1. 事件定级

从以上的安全事件分类分析可知，不同的安全事件对系统可用性、安全性造成的破坏，严重程度不同。这里根据系统可用性和安全性遭受破坏的程度，对以上安全事件进行定级，分为一般事件、紧急事件、严重事件共三级。

* 1. 一般事件（I级）

一般事件只对系统可用性造成轻微破坏，稍加修正即可使系统恢复正常使用。一般事件不会影响到系统的安全性，主要包括：

① 业务系统密码应用集成故障

② 密码产品部署故障

③ 系统管理员证书失效

* 1. 紧急事件（II级）

紧急事件发生时能马上影响到系统可用性，且修复起来有一定的难度，但不会影响到系统的安全性，主要包括：

① 业务系统服务器证书失效

② 服务端密码设备故障

* 1. 严重事件（III级）

严重事件指能够影响到系统的安全性，主要包括：

① 业务系统密码应用集成漏洞

② 服务端密钥泄露

③ 密码设备的安全漏洞

6.7.2 应急处置组织机构与职责

1. 密码服务组织机构

测试项目A应结合其日常组织机构建立密码服务应急响应的组织机构，并明确其职责。其中一些人可负责两种或多种职责，一些职位可由多人担任（应急响应计划文档中应明确他们的替代顺序）。

应急响应的组织机构由管理、业务、技术和行政后勤等人员组成，一般可设为应急响应领导小组、应急响应实施小组和应急响应日常运行小组等。组织可聘请具有相应资质的外部专家协助应急响应工作，也可委托具有相应资质的外部机构承担实施小组以及日常运行小组的部分或全部工作。在聘请外部专家协助应急响应工作或者委托外部机构承担部分或者全部应急工作时需要和其签订相关协议（例如签订有关信息保密要求等）。

1. 应急响应领导小组

测试项目A应组建应急响应领导小组，应急响应领导小组是信息安全应急响应工作的组织领导机构，组长应由组织最高管理层成员担任。领导小组的职责是领导和决策信息安全应急响应的重大事宜，主要如下：

* 1. 审核并批准经费预算
  2. 审核并批准恢复策略
  3. 审核并批准应急响应计划
  4. 批准应急响应计划的执行

1. 应急响应日常运行小组

应急响应日常运行小组的主要职责是：

* 1. 协助恢复密码服务的实施
  2. 备份中心密钥管理
  3. 管理信息系统的运行的密码服务设备
  4. 密码服务灾难恢复的专业技术支持
  5. 参与和协助密码服务应急响应计划的教育、培训和演练
  6. 维护和管理应急响应商用密码服务计划文档
  7. 密码服务突发中止事件发生时的损失控制和损害评估
  8. 密码服务中止发生后的恢复
  9. 密码服务中止发生后的外部协作

1. 应急响应厂商

应急响应厂商的主要职责是：

* 1. 协助恢复密码服务的实施
  2. 密码服务的专业技术支持
  3. 参与和协助商用密码服务应急响应计划的教育、培训和演练
  4. 密码服务中止发生后的恢复

6.7.3 应急处置预案设计

针对潜在的安全事件，进行了应急处置预案的设计。

1. 项目实施过程中的安全事件应急处置预案

针对项目实施过程中的安全事件，应急处置预案设计如下，包括系统密码应用集成故障、密码产品部署故、密码应用集成漏洞。

* 1. 系统密码应用集成故障，如表 6.1所示。

表6.1 系统密码应用集成故障

|  |  |
| --- | --- |
| 出现问题的原因 | 因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统无法正常使用密码产品的事件。 |
| **问题影响** | 密码应用在业务的生产系统验证失效 |
| **事前防范** | 上线生产前做多次模拟生产运行的验证测试 |
| **事中处理** | 进行密码应用算法回退；  进行数据恢复。 |
| **事后处置** | 校验模拟系统和生产系统间的差异；  充份分析所遇到的问题细节；  待所有问题解决后再进行二次上线验证。 |
| **损失评估** | 延误了系统密码算法安全性整体更新的进度 |

* 1. 密码产品部署故障，如表 6.2所示。

表 6.2 密码产品部署故障

|  |  |
| --- | --- |
| 出现问题的原因 | 因密码产品实施人员工作疏忽，造成密码产品无法正常工作的事件。 |
| **问题影响** | 上线生产后密码产品设备不工作或工作异常 |
| **事前防范** | 上线生产前充份验证设备配置文档，并且多次做模拟生产上运行环境的压力测试和功能测试 |
| **事中处理** | 进行密码应用算法回退；  密码产品部署回退，定位问题。 |
| **事后处置** | 分析模拟系统和生产系统间的差异；  全面分析失败上线的原因；  待所有问题解决后再进行二次上线，验证。 |
| **损失评估** | 延误了系统密码算法安全性整体更新的进度 |

* 1. 密码应用集成漏洞，如表 6.3所示。

表 6.3 密码应用集成漏洞

|  |  |
| --- | --- |
| 出现问题的原因 | 因业务系统开发商的工作疏忽或对密码产品接口掌握不全，造成业务系统密码应用存在漏洞的事件，典型的有：身份鉴别时对证书有效性验证不严谨，造成已过期的、被注销的、非受信CA颁发的证书可以通过认证；身份鉴别时没有采用随机数签名，造成身份鉴别信息可被重放攻击等 |
| **问题影响** | 有心攻击信息的黑客很容易蒙混到信息系统内部，引发内部信息泄漏风险 |
| **事前防范** | 技术上对认证的原理进行了理论性的认证，并给出了集成的拓扑说明；  可复制参考的集成示例，接口介绍文档；  宽且广的测试案例的覆盖。 |
| **事中处理** | 系统全面回退到使用证书登录前的状态；  待所有问题解决后再进行二次上线，验证。 |
| **事后处置** | 开发人员重新参考方案，做原理层的深入了解，充分理解示例代码，接口说明文档；  重新做证书认证产品的接入；  宽且广的测试案例的覆盖，β测试。 |
| **损失评估** | 延误了强身份认证的上线进度，给系统安全性存在身份认证方面的不足，容易受到黑客密码穷举，撞库等方面的攻击，存在内部信息泄漏的风险。 |

1. 密码运行过程中出现的安全事件应急处置预案

针对密码运行过程中的安全事件，应急处置预案设计如下，包括系统管理员证书失效、系统服务器证书失效、密钥泄漏、密码设备故障、密码设备的安全漏洞。

* 1. 系统管理员证书失效，如表 6.4所示。

表 6.4 系统管理员证书失效

|  |  |
| --- | --- |
| 出现问题的原因 | 系统管理员证书在过期前没有及时去续期、系统管理员证书介质PIN锁死或介质损坏。 |
| **问题影响** | 系统管理员无法正常登录业务系统进行维护和管理工作，对业务系统的可用性可能会造成影响。 |
| **事前防范** | 设立规范制度要求：管理员每个月定期查看系统管理员证书的有效时间，设置两个管理证书介质互为备份。 |
| **事中处理** | 采用备份的管理证书介质登录系统；  使用备份的管理员介质做常用的系统管理员的新证书。 |
| **事后处置** | 加强规范制度的落实措施；  强调备份的重要性，备份的使用周期要比应用中的产品周期长1.5-2倍。 |
| **损失评估** | 管理员登录不及时导致系统维护不及时，造成密码服务的连续性服务中断。 |

* 1. 系统服务器证书失效，如表 5.6所示。

表 6.5 系统服务器证书失效

|  |  |
| --- | --- |
| 出现问题的原因 | 业务系统的服务器证书在过期前没有及时去续期；业务系统IP或域名修改没有及时申请新的IP或域名证书。 |
| **问题影响** | 服务器证书验证失败，影响业务系统的正常访问 |
| **事前防范** | 设立规范制度要求管理员每个月定期查看服务器的有效时间，确定服务器证书可继续服务的时间。  系统的任意修改需要做出风险评估后，落实准备条件再做切换或更改。 |
| **事中处理** | 针对证书过期问题，一方面管理员需要尽快为过期的服务器证书续期；另一方面向CA机构申请临时服务器证书过渡网站正常应用。  没有及时申请新问题，采用IP或域名回退机制，待新证书申请下来后再做IP或域名的切换。 |
| **事后处置** | 加强规范制度的落实措施；  加强从测试到生产的验证性测试。 |
| **损失评估** | 影响信息系统的IP或域名切换进度，临时证书申请过程和机制回退造成密码服务的连续性服务中断。 |

* 1. 密钥泄漏，如表 6.6所示。

表 6.6 密钥泄漏

|  |  |
| --- | --- |
| 出现问题的原因 | 服务端的服务器密码机、签名验签服务器设备里的密钥（包括私钥、对称密钥、MAC密钥）泄漏事件。 |
| **问题影响** | 关键敏感数据存储与传输的私密性、完整性被破解 |
| **事前防范** | 密钥对应的信息系统应用模块做好登记；  多套密钥同时运行。 |
| **事中处理** | 评估密钥泄漏可能波及到的系统范围；  在密码服务系统中采用新的一套密钥；  信息系统尽快做好密钥切换工作与新密钥验证；  销毁旧密钥，做好新密钥的备份措施和安全控制措施。 |
| **事后处置** | 追踪密钥外泄的原因；  加强制度的管理；  强化密钥管理安的全意识。 |
| **损失评估** | 密钥外泄的信息系统数据存在泄漏的风险 |

* 1. 密码设备故障，如表 6.7所示。

表 6.7 密码设备故障

|  |  |
| --- | --- |
| 出现问题的原因 | 服务端的服务器密码机、签名验签服务器设备故障事件。 |
| **问题影响** | 业务系统身份鉴别、数据安全存储、数据安全传输等功能异常 |
| **事前防范** | 做好密码服务设备的双套运行备份；  做好密码服务设备的密钥备份。 |
| **事中处理** | 马上使用备用设备替换现有密码服务系统设备，隔离出问题的密码服务系统设备。  分析出问题的设备的原因，做好必要记录，妥善保存有关记录及日志或审计记录。  如果满足下列情况之一的，应立即向信息中心负责人通报情况，申请由应急响应小组协助处理：  密码服务系统设备在2小时内无法处理完毕的。  密码服务系统设备涉临淘汰，市场上无法找到替代密码服务的设备。  在应急响应小组协助修复设备后，进行密码系统和相关数据恢复，检查密码系统数据的完整性。  相关密码服务故障事件处理完毕，重新接入网络。 |
| **事后处置** | 总结事件处理情况，将有关情况向安全领导小组领导汇报有关情况，并提出防范再度爆发的解决方案。  配合应急响应小组实施必要的安全加固。 |
| **损失评估** | 主备机的切换影响密码连续性工作的中断 |

* 1. 密码设备的安全漏洞，如表 6.8所示。

表 6.8 密码设备的安全漏洞

|  |  |
| --- | --- |
| 出现问题的原因 | 服务器密码机、签名验签服务器、智能密码钥匙等密码设备存在软件或硬件上的安全漏洞事件。 |
| **问题影响** | 密码设备可以被非法访问、私钥可被猜测等安全问题 |
| **事前防范** | 及时根据密码服务设备厂家发布的漏洞进行补丁修复；  定期观查密码服务器的运行日志，把握密码设备的运行状态。 |
| **事中处理** | 及时根据密码服务设备厂家发布的漏洞进行补丁修复。 |
| **事后处置** | 加强与密码设备厂家的沟通，尽可能在漏洞公布后及时进行补丁修复；  评估漏洞事件可能带来的系统风险。 |
| **损失评估** | 密码设备可以被非法访问、私钥可被猜测等安全问题可能会导致用户数据外泄，安全数据泄漏的风险。 |

7 实施保障方案

根据《政务信息系统密码应用与安全性评估工作指南（2020版）》、《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》，结合信息系统的实际情况，项目预算及拟采购的密码产品，落实第5章密码应用技术方案和第6章密码安全管理方案，从实施内容、实施计划、保障措施三个方面设计实施保障方案，保障目标信息系统顺利、成功进行密码应用改造。

7.1 实施内容

目标信息系统密码应用的实施内容包括软硬件开发及改造、系统集成、综合调试、试运行、最终验收、风险点及应对措施六个方面。

7.1.1 软硬件开发及改造

按照采购内容和目标信息系统密码应用改造要求，对采购的密码软硬件进行定制开发和改造，以符合实现项目需求。

表7.1 定制开发任务表

|  |  |  |  |
| --- | --- | --- | --- |
| 指标要求 | 开发任务 | 信息系统模块 | 对接密码产品 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

7.1.2 系统集成

目标信息系统，通过集成密码产品中间件，业务应用系统提供密码服务和身份认证服务。

密码安全应用贯穿业务始终，即从传输链路、身份鉴别、数据加密、电子签名、数据完整性保护等方方面面。例如在用户在与服务端之间通信时，通过安全网关建立加密通道、数据进行存储时以密文的形式存储、对访问控制策略信息进行HMAC运算和校验、对用户操作行为使用用户的证书进行签名/服务端发出的数据可以由应用系统自身的数字证书进行签名等，充分保证了应用系统的使用安全。

7.1.3 综合调试

系统集成完成后，密码软硬件产品上架部署后，进行统一的综合调试，串通整体业务流程和密码应用流程。

7.1.4 试运行

系统移交买方后即进入试运行阶段，试运行时间为1个月，试运行期间卖方负责解决问题清单中的遗留问题，进一步完善系统，并且在此过程中，卖方应提供完善的监护服务。

试运行结束后，由卖方负责起草《试运行报告》，经双方确认并签署。

7.1.5 最终验收

系统在试运行期结束后进行工程终验，需由卖方提出终验书面申请，且买方需在收到卖方终验申请后10个工作日内组织工程终验。若10日内买方没有响应或无正当理由推迟，则视为系统通过终验。

测试项目一般同初步验收测试相同，考虑到测试进度的因素，系统终验可以只对对初验遗留的问题进行测试验证，对初验通过的免予测试。验收通过后，卖方应提供相应的工程文档，工程文档应包括：系统详细配置说明书、软件安装测试记录、使用及维护说明书、所有软件的文档等。

终验通过后，由卖方负责起草《系统终验合格证明》，经双方确认并签署。

7.1.6 风险点及应对措施

风险管理贯穿于整个项目实施过程，通过制定项目实施过程的风险管理计划，并在项目各生命周期阶段开始时进行相应的评估，在项目实施过程中持续进行风险识别、监控、处理，最终把实施阶段的风险控制在可以接受的范围。本项目实施和运行过程中主要存在的风险包括：

1. 外部风险分析及对策

外部风险主要是由于外部不可控因素造成的风险。一般将不可控制的“不可抗力”不作为风险因素处理，这些事件往往采用灾难防御措施。对于此项目，要做好在政策法规、外部资源、技术等方面的风险防范。

项目中的外部风险主要包括如下几类：

* 1. 外部资源风险

**外部资源风险：**由于外部资源因某种原因无法按计划配置，导致总体进度受到影响，如承包商无法按原计划完成项目软硬件建设、项目实施时与原应用开发商无法对接等情况。

**风险对策：**尽早识别关键性的外部资源，与资源的提供方进行沟通，并提前配置或增加足够的备份方案。通过招标方式，选择具备资质、有类似项目实施经验的软硬件承包商，深入了解各个软硬件建设方案的优缺点及应急措施；对于关键性数据，需明确其来源，并尽快安排与应用开发商进行沟通协调。

* 1. 标准风险

**标准风险：**国家和行业出台了新的业务标准或技术标准，与项目所执行的标准不一致，导致前期的规划失效。

**风险对策：**严格按照国家出台的相关标准制定系统建设框架，制定项目的业务标准和技术标准，符合密码发展的趋势。

**在标准设定时：**严格按照调研、需求分析、审核、征询建议、整合、征询建议、审核、标准制定、备案、更新现有标准体系、产生新版本的标准规范、对旧版本的标准规范存档、发布新标准的流程进行。

1. 内部风险分析及对策

内部风险主要是项目实施过程中，由于组织管理缺失、项目管理不当所导致的项目无法顺利开展的风险。充分地认识、正确地处理内部风险将会是保证项目最终成功的关键。

项目中的内部风险主要包括如下几类：

* 1. 组织风险

**组织风险：**组织风险主要指组织内部成员对目标未达成一致，管理高层对项目不重视，加上工程参与人员知识与技能欠缺、团队合作精神不足、人员激励机制不当等因素导致建设队伍不稳定，与其它项目存在资源冲突等。

**风险对策：**本次项目充分考虑到了项目中的组织风险，根据信息化系统的建设要求，在充分论证的基础上完善信息化建设项目的完整架构，保证信息化建设项目的正常运转，包括部门设置、岗位确定、职责落实、人员配备、制度建立等内容，将有效地保障目标信息系统项目建设中避免组织风险的发生。

* 1. 管理风险

**管理风险：**管理风险主要包括项目管理的基本原则使用不当，如计划草率、质量差、进度和资源配置不合理等。

**风险对策：**为确保项目管理的高效率，本项目建设领导小组将对项目建设方案进行有效策划，制定并落实严格的项目实施具体计划，应用先进管理工具和方法论提高进度计划管理、跟踪水平。借鉴同行业项目管理的实际经验，合理估算项目工作量，明确项目间依赖关系和先后顺序，突出关键项目，进一步分解项目工作任务，使每个里程碑阶段均应有工作量估算、时间进度，以及可操作、可管理、可检查的阶段性交付物。

为了避免在项目建设过程中对实施方的管理、协调不力，项目建设领导小组将制订统一的标准、流程和规范，并加强全过程的质量控制，在招标书、合同等文件中明确服务商应遵循的质量管理体系，明确项目工作范围，明确系统边界、需求、约束等前置条件。选择具备资质的监理单位，对项目实施过程中的工程招标、工程设计、工程实施、工程验收等项目建设全过程的进度、质量、投资、变更等行为进行监督和管理。

7.2 实施计划

目标信息系统密码应用的实施计划包括实施路线图以及进度计划两个方面。

7.2.1 实施路线图

根据本项目的需求，编制《项目建设实施方案》，组织专家进行评审论证，并报领导小组备案，报请用户批准；在《项目建设实施方案》被批准后，将严格按照实施方案、时间进度要求，组织工程建设，完成工程建设任务，组织工程验收，系统投入运行。

本项目具体实施主要包括以下几个步骤：

1. 组建项目实施团队；
2. 制定实施计划、编制《项目建设实施方案》；
3. 项目实施安装，进行软硬件的安装与调试；
4. 项目培训；
5. 系统试运行与交付；
6. 系统正式运行；
7. 日常运维。

7.2.2 进度计划

本项目主要阶段实施工作分解如表7.2所示：

表7.2 阶段实施工作分解表

|  |  |  |
| --- | --- | --- |
| 时间计划 | 工作阶段 | 工作内容 |
|  | 需求调研分析 | 根据需求调研计划，结合前期需求调研情况，针对信息系统的国产密码应用情况进行详细调研，并形成关于国产密码应用的《需求规格说明书》和《需求确认书》。 |
|  | 安全方案设计 | 基于用户单位建设方案及实际情况，设计密码系统部署、密码系统与应用对接、网络拓扑、安全防护机制和备份恢复机制等，确定设备配置，拟定详细建设方案。 |
|  | 项目准备启动 | 熟悉项目前期所形成的资料，制定项目实施计划，确定项目组织架构及人员，成立项目管理办公室，制定项目启动会议计划，召开项目启动会议。 |
|  | 项目研发 | 项目详细方案评审通过后，密码厂商即刻展开密码系统功能详细设计，按系统功能，进行相应模块的开发，并形成《详细设计说明书》。 |
|  | 项目测试 | 针对项目实施内容，编制产品测试方案、密码系统产品与改造后信息系统的联调测试、编制测试评估报告  项目试运行：测试完成通过进入项目试运行阶段，在试运行阶段遇到问题密码厂商需及时解决并对问题进行记录，形成问题知识库。 |
|  | 培训与交付 | 为项目用户单位编写技术参数手册和工程安装手册。编写培训方案，对试点信息系统相关人员进行全面的技术和运维培训，并生成培训记录和反馈。 |
|  | 密码测评 | 在建设完成后，通过密码测单位进行密码测评，并出具测试报告 |
|  | 项目试运行 | 进行系统试运行 |
|  | 项目验收 | 制定验收方案并完成系统验收工作 |

7.3 保障措施

目标信息系统平台密码应用的保障措施包括组织保障、人员保障、经费保障、质量保障四个方面。

7.3.1 组织保障

1. 组织架构

本项目实施过程中，组织一整套的开发、工程人员，组建专业的研发、工程施工和服务队伍，力求为该项目提供最为完善的工程支持，项目的组织架构如图 7.1所示。

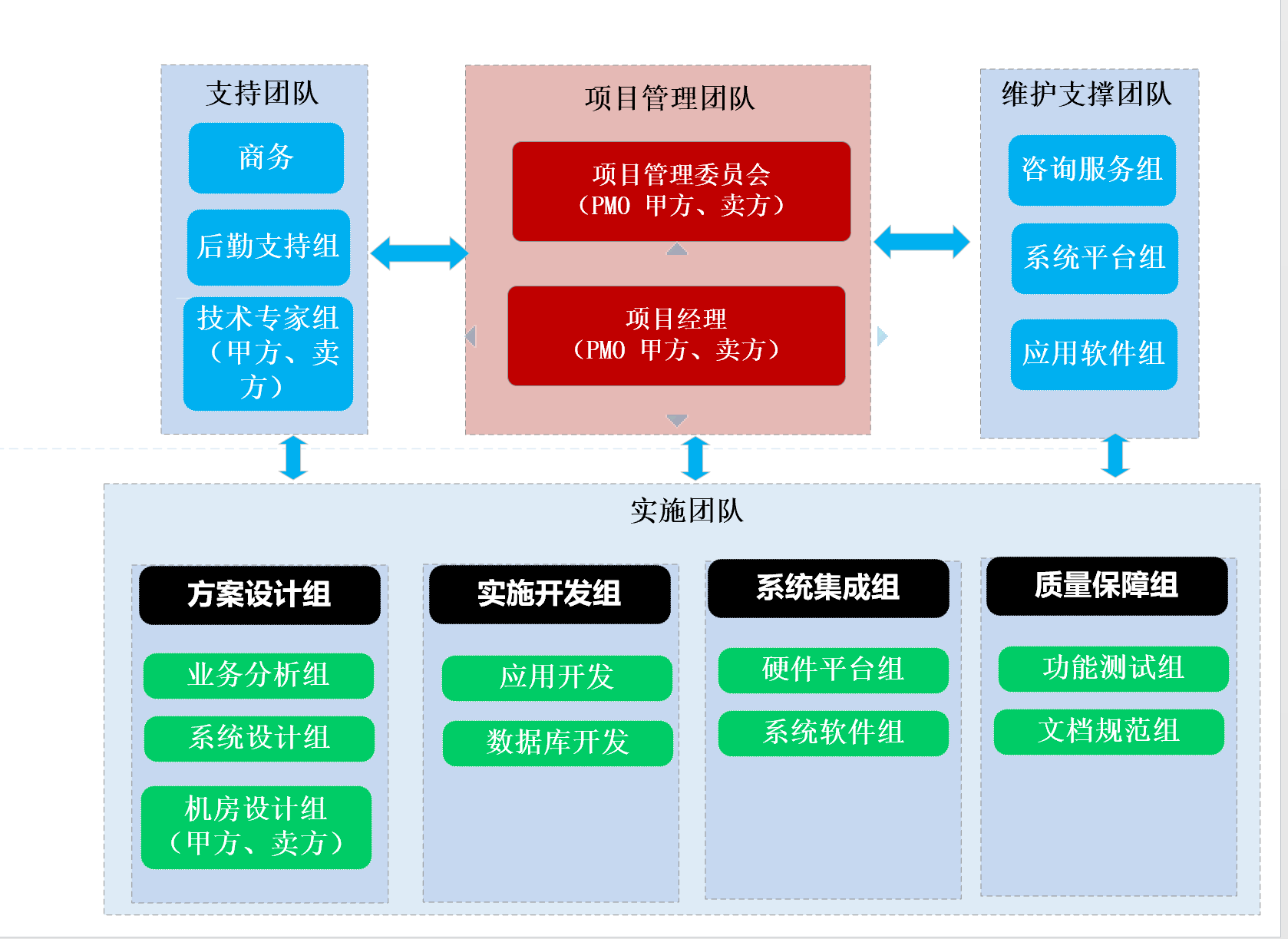


图 7.1 组织架构图

1. 项目管理团队

项目管理团队负责对项目进度、工程质量进行宏观管理，提供对项目出现的重大问题进行协调和指导，完成重要阶段评审，与项目内外部人员及合作方进行沟通，确保项目顺利成功实施。

项目管理团队包括以下角色：

* 1. 项目管理委员会：负责从商务角度对项目发展方向、管理策略、资源调配等进行决策，并有权任免以下层次人员组成。管理委员会成员由甲方、卖方人员组成；
  2. 项目经理：负责从项目运作角度协调管理，支持项目实施团队工作，向管理层汇报，对项目成败负责。项目经理成员由甲方、卖方人员组成。

1. 实施团队

实施团队负责系统平台集成和建设实施，对于项目最终产出提交物负责。

实施团队包括以下角色：

* 1. 方案设计组：对系统的建设进行设计规划，包括了业务分析设计和系统分析设计两部分。
  2. 业务分析组：负责收集、分析、汇总用户需求，与系统设计组及实施开发组配合工作；
  3. 系统设计组：负责从系统架构和技术选型角度进行分析设计，建立系统逻辑模型，从而指导实施开发组工作；
  4. 机房设计组：配合买方负责对整体机房做整体建设设计，输出建设图纸。
  5. 实施开发组：负责从系统实施角度进行代码开发，完成软件模块的开发、修改和整合。
  6. 应用开发组：负责除数据库开发外的代码开发内容，包括界面操作逻辑、业务逻辑和接口等；
  7. 数据库开发组：负责对数据库操作部分的开发实施工作，对应用开发组予以技术支持。
  8. 系统集成组：负责设备平台的架设、安装、调试，同时将开发完成的软件有效的集成发布在测试、生产环境，并确保调试通过。
  9. 硬件平台组：负责设备平台的架设安装及调试工作；
  10. 系统软件组：负责系统软件及第三方软件的发布和调试，并配合实施开发组对开发完成的应用在测试和生产环境进行发布，并确保调试通过；
  11. 机房建设组：配合买方对机房建设提供必要的支持。
  12. 质量保障组：负责从质量管理角度，定制适合本项目应用的工作流程，同时定期实施质量审核，以确保整个项目的质量水平。
  13. 功能测试组：负责对整个系统进行软硬件测试，完成测试文档，并及时将所发现的问题向有关的部门通报；
  14. 文档规范组：负责汇总并整理相关工程技术文档，提交有关责任人审核通过，同时管理各类技术规范和资料库，支持项目其他团队工作。

1. 维护支撑团队

维护支撑团队负责系统的维护优化，并保证生产环境的正常工作。同时，维护支撑团队也面向用户提供咨询、培训和技术支持。

维护支持团队包括以下角色：

* 1. 咨询服务组：就系统运行维护相关的主题，提供各类咨询服务以及培训支持；
  2. 系统平台组：从设备平台的角度提供运行维护支持，以及有关系统的性能调优；
  3. 应用软件组：从应用软件的角度提供运行维护支持，以及相关功能的优化开发。

1. 支持团队

支持团队负责提供与本项目相关的外部支持，包括了商务合作、后勤保障、专家咨询等。支持团队包括以下角色：

* 1. 商务合作部：负责落实与项目相关的商务运作，主要包括设备订购。跟踪设备的到货情况，确保设备按期、准确、全部到达。同时，也可对客户提出的其他商务合作要求提供支持；
  2. 后勤支持组：负责整个项目的后勤支持，安排项目人员的工作环境和起居安排，减少项目组的无效投入；
  3. 技术专家组：从技术角度对整个项目提供支持，制定并审核本项目中的技术实施方案，解答技术问题，处理工程中出现的技术难点，必要时组织团队进行技术攻关。技术专家组成员由甲方、卖方人员组成。

7.3.2 人员保障

为确保项目的顺利开展、实施和运维，严格按照7.3.1设置的组织结构组织项目组人员，并按照一定的比例设置AB角。

7.3.3 经费保障

由项目建设方负责本项目资金的筹措和分配实施，详见7.4经费概算。

7.3.4 质量保障

1. 建立软件质量保证活动的实体

建立软件质量保证小组，软件质量保证小组在整个软件生命周期中应评审项目的活动并审计软件工作产品，使管理层能观察到软件项目是否遵从已建立的计划、标准和规程。并应指出在该软件项目中的问题：如果可能，则应及时解决；如果不能解决，则应提交到适当的管理层解决。

1. 制订软件质量保证计划

SQA计划应在整个项目的早期制订，并应与整个项目计划平行开发。 此计划包括：

* 1. SQA小组的职责和权利。
  2. SQA小组的资源需求（包括人员，工具及设施）。
  3. 该项目的SQA小组活动的进度安排和经费。
  4. SQA小组参与建立该项目的软件开发计划、标准和规程。
  5. 由SQA小组进行评估的内容。
  6. 由SQA小组指导的审计和评审。
  7. SQA小组在评审和审计时引用的项目标准和规程。
  8. 记录和跟踪不协调事项直至解决的规程。
  9. 要求SQA小组生成的文件。
  10. 为软件工程小组和其他软件相关小组提供SQA活动反馈信息的方法和频率。

1. 坚持各阶段的评审和审计，并跟踪其结果作合适处理
   1. 评审：包括里程碑活动评审、基线评审、SCM评审、SQA工作评审。
   2. 审计：包括基线审计、SQA审计。

有背离之处，则对其进行标识、记录、并跟踪直至其符合。

1. 监控软件产品的质量
   1. 对软件产品的验收
   2. 把握采购软件的质量
   3. 监控分承包商的软件质量保证工作
2. 采集软件质量保证活动的数据
   1. 记录不协调事项
   2. 跟踪不协调事项直至解决
   3. 收集各阶段的评审和审计情况
3. 度量软件质量保证活动
   1. 测量的目的是为了判断SQA活动的成本和进度状态；
   2. 与其计划相比，SQA活动完成的里程碑数；
   3. 在SQA活动中完成的工作，花费的工作量及支出的费用；
   4. 与其计划相比，产品审计和活动评审的次数。
4. 软件质量保证管理流程

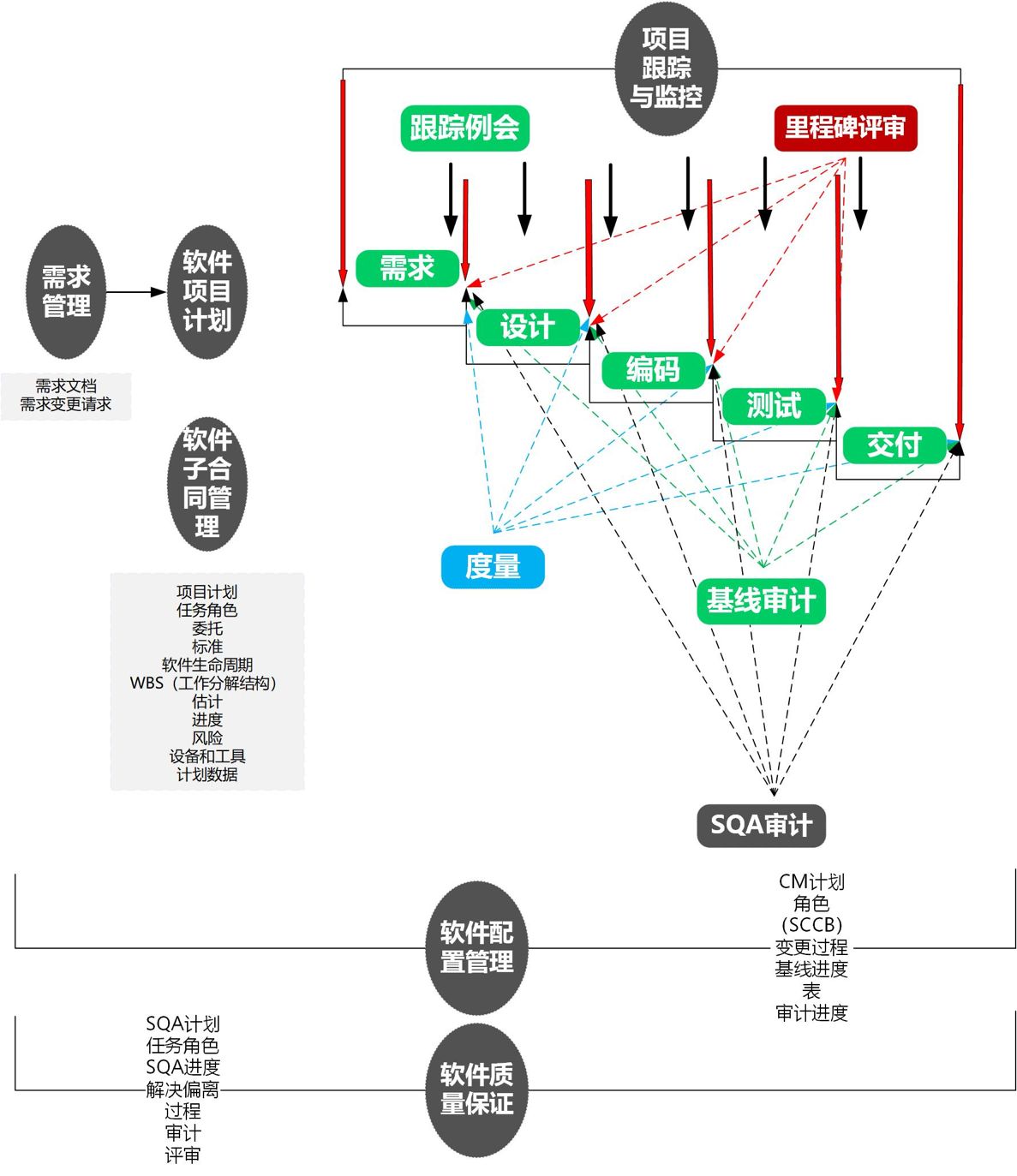


图 7.2 软件质量保证管理流程图

软件质量保证管理流程如图 7.2所示，首先设定需求管理和软件项目计划，依次从需求、设计、编码、测试、交付五个阶段展开项目跟踪与监控，监控软件产品的质量，采集软件质量保证活动的数据；同时坚持各阶段的评审和审计，并跟踪其结果作合适处理，有背离之处，则对其进行标识、记录、跟踪直至其符合。