普洱公积金综合服务平台密码应用方案

项目名称： 普洱公积金综合服务平台

项目建设单位： 普洱市住房公积金管理中心

编制日期：2024年07月11日

**目录**

[1背景 1](#_Toc167377439)

[1.1系统的建设规划 1](#_Toc167377440)

[1.2国家有关法律法规要求 1](#_Toc167377441)

[1.3与规划有关的前期情况描述 4](#_Toc167377442)

[1.4项目实施的必要性 5](#_Toc167377443)

[2系统概述 7](#_Toc167377445)

[2.1基本情况 7](#_Toc167377446)

[2.2计算平台现状 9](#_Toc167377447)

[2.3业务应用现状 13](#_Toc167377448)

[2.4密码应用现状 16](#_Toc167377449)

[2.5密码应用管理现状 18](#_Toc167377450)

[3. 密码应用需求分析 18](#_Toc167377451)

[3.1计算平台 19](#_Toc167377452)

[3.2业务应用 30](#_Toc167377453)

[3.3安全管理 34](#_Toc167377454)

[4. 安全目标及设计原则 35](#_Toc167377455)

[4.1安全目标 35](#_Toc167377456)

[4.2设计原则与依据 35](#_Toc167377457)

[5. 密码应用设计 37](#_Toc167377458)

[5.1密码应用技术框架 37](#_Toc167377459)

[5.2计算平台密码应用方案 44](#_Toc167377460)

[5.3密码支撑平台方案 53](#_Toc167377461)

[5.4业务应用密码应用方案 60](#_Toc167377462)

[5.5密码应用部署 71](#_Toc167377463)

[6. 安全管理方案 74](#_Toc167377464)

[6.1管理制度 74](#_Toc167377465)

[6.1 密码安全管理制度 75](#_Toc167377466)

[6.2 人员管理 78](#_Toc167377467)

[6.3 密钥管理 81](#_Toc167377468)

[6.4 建设运行 83](#_Toc167377469)

[6.5 密码软硬件及介质管理 84](#_Toc167377470)

[6.6 应急方案 86](#_Toc167377471)

[7. 安全与合规性分析 94](#_Toc167377472)

[8. 实施保障方案 99](#_Toc167377473)

[8.1 实施内容 99](#_Toc167377474)

[8.2实施计划 104](#_Toc167377475)

[8.3保障措施 106](#_Toc167377476)

[8.4经费概算 112](#_Toc167377477)

# 1 背景

## 1.1系统的建设规划

## 1.2国家有关法律法规要求

### 1.2.1《中华人民共和国密码法》

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》，习近平主席签署第35号主席令予以公布，于2020年1月1日起正式施行。

根据密码法第二条的规定，本法中的密码，是指采用特定变换的方法对信息等进行加密保护、安全认证的技术、产品和服务。密码是保障网络与信息安全的核心技术和基础支撑，是解决网络与信息安全问题最有效、最可靠、最经济的手段，在我国革命、建设、改革各个历史时期，都发挥了不可替代的重要作用。密码就像网络空间的DNA，是构筑网络信息系统免疫体系和网络信任体系的基石，直接关系国家政治安全、经济安全、国防安全和信息安全，是保护党和国家根本利益的战略性资源，是国之重器。

在商用密码使用方面，一方面，为了保障关键信息基础设施安全稳定运行，维护国家安全和社会公共利益，密码法第二十七条要求关键信息基础设施必须依法使用商用密码进行保护并开展商用密码应用安全性评估，要求关键信息基础设施的运营者采购涉及商用密码的网络产品和服务，可能影响国家安全的，应当依法通过国家网信办会同国家密码管理局等有关部门组织的国家安全审查。另一方面，密码法第八条规定公民、法人和其他组织可以依法使用商用密码保护网络与信息安全。

### 1.2.2《广东省省级政务信息化项目管理办法》（广东省特有）

为进一步落实“数字政府”改革建设工作任务，理顺政务信息化管理体制，推进“数字政府”管运分离建设模式，实现政务信息化项目由条块化管理向整体化管理转变、由政府投资建设向购买服务转变，根据广东省“数字政府”改革建设要求，2020年4月，《广东省省级政务信息化项目管理办法》正式印发。相关章节说明如下：

第九条省政务服务数据管理局依托管理平台牵头建立政务信息系统目录动态管理机制。具有以下情形之一的，相关运行维护、运营以及升级项目原则上不予立项。

（一）未纳入政务信息系统目录的系统；

（二）未按要求共享数据资源或者重复采集数据的政务信息系统；

（三）不符合密码应用和网络安全要求，或者存在重大安全隐患的政务信息系统；

（四）不符合国家安全可靠应用政策的政务信息系统。

### 1.2.3《网络安全等级保护条例（征求意见稿）》

第二十条“网络运营者应当落实数据分类、重要数据备份和加密等措施”；第四十七条“【非涉密网络密码保护】非涉密网络应当按照国家密码管理法律法规和标准的要求，使用密码技术、产品和服务”。

第三级以上网络运营者应在网络规划、建设和运行阶段，按照密码应用安全性评估管理办法和相关标准，委托密码应用安全性测评机构开展密码应用安全性评估。网络通过评估后，方可上线运行，并在投入运行后，每年至少组织一次评估。密码应用安全性评估结果应当报受理备案的公安机关和所在地区市的密码管理部门备案。

### 1.2.4《商用密码应用安全性评估管理办法》

第六条 法律、行政法规和国家有关规定要求使用商用密码进行保护的网络与信息系统（以下简称重要网络与信息系统），其运营者应当使用商用密码进行保护，制定商用密码应用方案，配备必要的资金和专业人员，同步规划、同步建设、同步运行商用密码保障系统，并定期开展商用密码应用安全性评估。

第八条 重要网络与信息系统建设阶段，其运营者应当按照通过商用密码应用安全性评估的商用密码应用方案组织实施，落实商用密码安全防护措施，建设商用密码保障系统。重要网络与信息系统运行前，其运营者应当自行或者委托商用密码检测机构开展商用密码应用安全性评估。网络与信息系统未通过商用密码应用安全性评估的，运营者应当进行改造，改造期间不得投入运行。

### 1.2.5《商用密码管理条例》

第四十一条 网络运营者应当按照国家网络安全等级保护制度要求，使用商用密码保护网络安全。国家密码管理部门根据网络的安全保护等级，确定商用密码的使用、管理和应用安全性评估要求，制定网络安全等级保护密码标准规范。

第四十二条 商用密码应用安全性评估、关键信息基础设施安全检测评估、网络安全等级测评应当加强衔接，避免重复评估、测评。

## 1.3与规划有关的前期情况描述

普洱公积金综合服务平台为新建系统，目前处于建设规划阶段。在建设过程中需根据系统的业务用户以及关键业务数据，明确保护对象，分析其密码应用的需求；为保障用户身份的真实性，业务系统的数据真实性、完整性和有效性，需要按GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的要求编制密码应用方案，进行密码应用建设。

## 1.4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》，决定对普洱公积金综合服务平台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。

通过对某信息系统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，普洱公积金综合服务平台安全性要求，就成为了重中之重。某信息系统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

2.1基本情况

2.1.1系统名称

普洱公积金综合服务平台

2.1.2系统责任主体单位

建设单位名称：普洱市住房公积金管理中心

地址：测试地址

所属密码管理部门：测试部门

单位类型：测试类型

2.1.3系统上线运行时间

2024年6月17日

2.1.4系统用户情况

| **序号** | **用户角色** | **业务场景** | **网络访问位置** |
| --- | --- | --- | --- |
|  | 运维人员 | 普洱公积金综合服务平台 | 互联网, 内网 |
|  | 系统管理员 | 普洱公积金综合服务平台 | 内网 |
|  | 普通用户 | 普洱公积金综合服务平台 | 内网, 互联网 |
|  | 公众用户 | 普洱公积金综合服务平台 | 互联网 |

2.1.5关键基础设施说明

已认定为关键信息基础设施，所属安全保护工作部门为测试部门。

2.1.6网络安全等级保护情况

系统等保定级：等保三级

备案时间：

备案号：

网络安全等级测评情况：正在测评，测评机构名称：测试名称。

2.1.7密码应用安全性评估情况

正在评估，密评机构名称：测试评估。

2.1.8部署情况

【云平台部署】云平台名称：测试云平台，云平台已评估，密评机构名称：测试云平台机构；评估时间：测试时间，评估结论：测试结论。

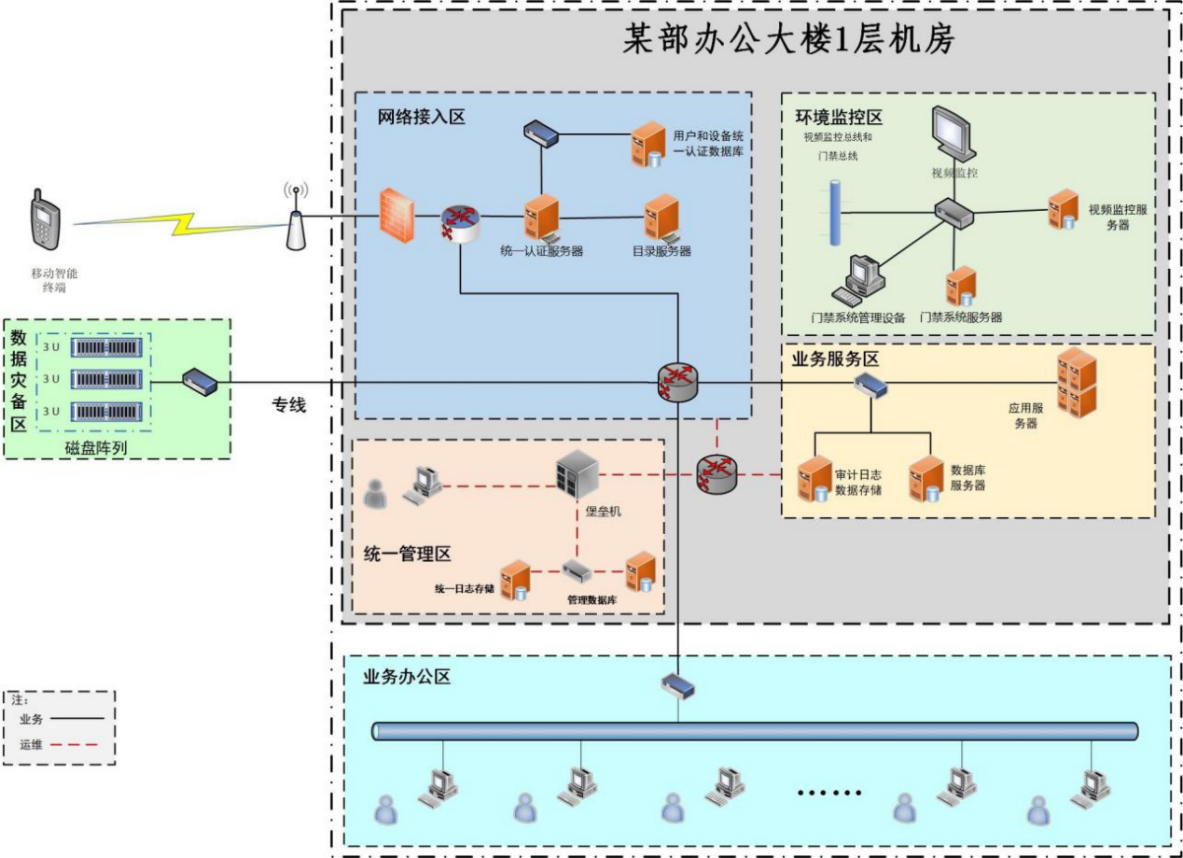
2.2计算平台现状

2.2.1物理环境现状

本系统部署在中心机房，地址为中心机房地址。机房安装有门禁和视频监控系统，门口有专人值守，且进出机房需要实名登记。机房管理责任主体单位为中心机房主体单位，机房外部所在大楼（园区）为运营商所有，由运营商管理。

2.2.2网络环境现状

系统网络划分为网络接入区、业务服务区、 统一管理区、 环境监控区、业务办公区、数据灾备区等六个区。系统网络安全防护符合等保2.0 相关要求。系统网络拓扑如下图1所示：



**图 1 系统网络拓扑图**

**网络接入区**位于政务网络边界，部署了统一认证服务器、数据库、目录服务器、交换机等设备，实现对接入用户和设备统一认证。

**业务服务区**是电子公文处理系统的核心服务区域，主要部署了电子公文处理系统应用服务器、数据存储服务器等设备，实现业务审批、公文签批、公文办理、 公文管理等业务过程的信息化管理。

**统一管理区**主要部署了远程运维管理终端、堡垒机、数据库等设备，实现对系统中的设备集中管理。

**环境监控区**主要部署了门禁系统和视频监控系统，实现对信息系统机房的物理安防管理。

**业务办公区**主要部署了办公终端、交换机等设备，实现我部办公人员通过我部政务办公网访问本系统。

**数据灾备区**主要部署了磁盘阵列等设备，实现重要业务数据的异地备份。

**内外部数据交互情况：**在内部数据交互过程中，用户在办公大楼局域网环境下，可通过部署在我部业务办公区的PC终端浏览器访问登录应用系统。运维人员使用运维终端在局域网，通过堡垒机实现统一集中运维管理。在外部数据交互过程中，用户在互联网环境下可通过移动智能终端访问登录应用系统；办公大楼1层机房业务服务器区通过专线将数据传输至灾备机房实现数据级灾备。

根据网络结构划分及数据交互情况，系统跨网络访问的信道有两个：①内部用户PC浏览器与业务系统之间的通信信道；②系统业务服务区和数据灾备区之间的专线通信信道；③公众用户移动端 APP与业务系统之间的通信信道；④XXX系统与业务系统之间的通信信道。

2.2.3计算环境现状

普洱公积金综合服务平台系统的软硬件设备情况如表2.7所示：

表 2.7 通用设备调查表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **设备名称** | **品牌型号** | **数量** | **操作系统** | **数据库** | **登录方式** |
| 综合数据库集群服务器1 | 华为 2488H V5 | 1 | Linux | Oracle | 用户名+口令, U盘证书 |
| 综合数据库集群服务器2 | 华为 2488H V5 | 1 | Linux | Oracle | 用户名+口令 |
| 综合服务平台服务器 | 华为 2488H V5 | 1 | Linux | Oracle | 用户名+口令 |
| 网厅服务器 | 华为 2488H V5 | 1 | Linux | Oracle | 用户名+口令 |
| 微信服务器 | 华为 2488H V5 | 1 | Linux | Oracle | 用户名+口令 |
| 转发服务器 | 惠普 HPProliantDL388Gen9 | 1 | Linux | Oracle | 用户名+口令 |
| 网站服务器 | 华为 2488H V5 | 1 | Linux | Oracle | 用户名+口令 |

普洱公积金综合服务平台系统的其他软硬件设备情况如表2.8所示：

表 2.8 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** | SSL VPN | 深信服 | 1 | 否 | 否 | 是 | 用户名+口令, U盘证书 | 是 |
|  | | | | | | | |
| **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)** | 无 |  |  |  |  |  |  |  |
|  | | | | | | | |
| **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** | 外网出口防火墙A | 山石网科 SG-6000-C400 | 1 | 否 | 否 | 是 | 用户名+口令, 手机短信 | 是 |
| 外网出口防火墙B | 山石网科 SG-6000-C400 | 1 | 否 | 否 | 是 | 用户名+口令, U盘证书 | 是 |
| 外网核心交换机A | 华为 S7703 | 1 | 否 | 否 | 是 | 用户名+口令 | 是 |
| 外网核心交换机B | 华为 S7703 | 1 | 否 | 否 | 是 | 用户名+口令, 手机短信 | 是 |
| 山石WEB防火墙 | 山石网科 SG-6000-W800 | 2 | 否 | 否 | 是 | 用户名+口令 | 是 |
| 日志审计 | 奇安信 LAS-R32P-PA | 1 | 否 | 否 | 是 | 用户名+口令 | 是 |
| 数据库审计 | 奇安信 DAS3000-TF10P | 1 | 否 | 否 | 是 | 用户名+口令 | 是 |
| 堡垒机 | 奇安信 C6100-BH-TF10 | 1 | 否 | 否 | 是 | 用户名+口令 | 是 |
| 运维发布服务器 | 山石网科 2288H-V5 | 1 | 否 | 否 | 是 | 用户名+口令 | 是 |
|  | | | | | | | |
| **虚拟设备和系统** | 无 |  |  |  |  |  |  |  |
|  | | | | | | | |

目前本系统运维管理员用户通过PC浏览器，使用账号+口令登录堡垒机，使用http协议与堡垒机之间建立安全连接，未使用密码技术对管理员登录进行身份鉴别，未使用合规的密码技术对进行远程管理的进行安全保护。

目前运维管理员接入堡垒机后，由堡垒机使用SSH协议与服务器之间建立远程管理通道，使用账号+口令登录服务器实现服务器及数据库的远程管理。未使用密码技术对登录服务器人员进行身份鉴别，未使用合规的密码技术对进行远程管理的进行安全保护。

目前堡垒机、服务器、数据库设备的重要程序或文件在生成时未使用密码技术进行完整性保护， 使用或读取这些程序和文件时，未对其进行完整性校验。设备的系统资源访问控制信息和日志记录均由设备自身明文存储，未使用密码技术进行完整性保护。

2.3业务应用现状

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：**

**业务应用现状包括以下具体描述。**

1. **业务应用的基本情况,包括承载的业务情况和责任主体等。**
2. **承载的业务情况,包括系统承载的业务应用、业务功能和关键数据类型等**
3. **对于多个子应用的信息系统,对每个子应用分别描述。根据系统实际情况，示例写法如下：**

2.3.1业务应用基本情况

XXX系统由A系统和B系统两个应用组成，其中A系统主要实现系统用户的统一身份认证。认证通过后用户进XXX系统应用，该应用主要为我部各级领导及办公人员提供业务审批、公文签批、公文办理、公文管理等业务过程的信息化管理，实现各部门之间横向与纵向业务流转和内部信息资源共享。XXX系统责任主体为我部，由我部对该系统进行运维管理。

2.3.2承载业务情况

2.3.2.1业务应用和功能

描述业务系统逻辑架构图和对应文字介绍。

（需提供逻辑架构图）

2.3.2.2关键数据类型

普洱公积金综合服务平台的应用层用户包括XXXXX员、XXXXX员、XXXXX用户、XXXXX用户。涉及的重要数据包括日志数据、鉴别数据和重要业务数据。重要业务数据包括：XXXX数据、XXXX数据、XXXX数据、XXXX数据。

系统涉及的关键操作有XXX。

XXXX系统的被保护对象信息如下：

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用名称 | 类别 | 具体保护对象 | 安全需求 |
| 1 | XXXXX系统 | 应用用户 | 系统管理员 | 真实性 |
| XXXX员 | 真实性 |
| XXXX员 | 真实性 |
| 重要数据 | 鉴别数据 | ☑传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 业务数据（XXXXXXX） | □传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 日志数据（用户登录、退出、操作日志等） | □传输机密性  □传输完整性  □存储机密性  ☑存储完整性 |
| 关键操作 | XXXXX行为 | 不可否认性 |
| ... | ... |
| N | XXXXX系统（根据实际，有子系统的按需求添加） | 应用用户 | 系统管理员 | 真实性 |
| XXXX员 | 真实性 |
| XXXX员 | 真实性 |
| 重要数据 | 鉴别数据 | ☑传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 业务数据（XXXXXXX） | ☑传输机密性  ☑传输完整性  ☑存储机密性  ☑存储完整性 |
| 日志数据（用户登录、退出、操作日志等） | □传输机密性  □传输完整性  □存储机密性  ☑存储完整性 |
| 关键操作 | XXXXX行为 | 不可否认性 |
| ... | ... |

2.4密码应用现状

系统当前未部署相关密码软硬件设施设备，未形成密码支撑功能供上层应用系统调用。本次密码应用方案通过后，我部将会依据方案部署相应密码密码软硬件设施设备，按照密码应用策略配置相关形成密码支撑功能。

2.4.1物理和环境安全现状

目前机房未采用合规的电子门禁系统和电子监控系统，未采用密码技术保证进出机房人员的身份鉴别，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和电子监控系统电子监控数据的存储完整性。

2.4.2网络和通信安全现状

服务通道采用HTTPS方式，通过政务外网对内部用户提供XXX服务，现阶段对内部PC端用户采用用户名+口令方式进行身份鉴别，未使用密码技术进行身份鉴别。对移动端用户采用测试方式方式进行身份鉴别，未使用密码技术进行身份鉴别。

2.4.3设备和计算安全现状

在运维侧，管理员用户通过堡垒机访问所需运维设备，使用用户名口令的方式对运维人员身份鉴别。通过HTTPS方式访问堡垒机，未使用合规的商密VPN技术进行远程管理通道的安全防护，相关日志未做完整性保护。

2.4.4应用和数据安全现状

现阶段业务系统包含多个子模块，涉及的系统开发语言是go，数据库类型是Oracle，数据库内数据现阶段明文存储，未采用合规的码技术保证信息系统应用的重要数据在传输和存储过程中的机密性和完整性。

2.5密码应用管理现状

普洱公积金综合服务平台，制定了三等密码安全制度，对涉及方面1、涉及方面2等进行了说明。

3.密码应用需求分析

**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：结合信息系统现状和GB/T39786中对不同等级的信息系统提出的密码应用基本要求,对密码应用方案涉及的计算平台、业务应用、管理制度、人员管理、建设运行和应急处置进行安全风险分析，确定风险控制措施、密码应用基本需求分析和密码应用特殊需求分析。通过风险控制措施缓解信息系统存在的高风险。根据系统实际情况，示例写法如下：**

3.1计算平台

3.1.1物理环境

物理环境风险分析

1、中心机房

1. 身份鉴别：机房门口部署了非国密电子门禁系统，未采用密码技术进行进入人员的身份鉴别，存在非法人员进入系统所在物理机房等重要物理环境，对软硬件设备和数据进行直接破坏的风险。
2. 电子门禁记录数据存储完整性：未采用密码技术对电子门禁系统的进出记录进行完整性保护，存在系统所在物理机房等重要物理环境电子门禁进出记录遭到篡改，非法人员进出情况被掩盖的风险。
3. 视频监控记录数据存储完整性：未采用密码技术对电子监控系统的视频监控记录数据进行完整性保护，存在系统所在物理机房等重要物理环境视频监控音像记录等遭到篡改，非法人员进出情况被掩盖的风险。

3、XXX机房（云机房）

【云平台通过了密评】该系统部署在XXX云，云平台已通过密码应用安全性评估，且安全等级不低于此信息系统，其密评报告中对云支撑能力进行了评估，本机房作为被完全评估的支撑能力，能同时支撑云平台和云应用在物理和环境安全层面的密码应用安全，采用云平台测评结论。

物理环境密码应用需求分析

{XXX机房已采用合规的电子门禁系统和电子监控系统，符合密评要求，无需改造。}

身份鉴别：采用缓解措施，基于生物识别技术（如指纹等）对重要区域进入人员进行身份鉴别；或（2）重要区域出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控。缓解措施可降低本指标的高风险程度。

电子门禁记录数据完整性：本方案中，不对电子门禁记录数据进行改造和完整性保护。

视频监控记录数据完整性：本方案中，不对视屏监控记录数据进行改造和完整性保护。

3.1.2网络环境

网络环境风险分析

系统在网络环境涉及以下两条通信信道：①内部用户PC浏览器与业务系统之间的通信信道；②系统业务服务区和数据灾备区之间的专线通信信道；③公众用户移动端 APP与业务系统之间的通信信道；④XXX系统与业务系统之间的通信信道。

1. 内部用户PC浏览器与业务系统之间的通信信道

身份鉴别：通过采用国际算法（算法如RSA2048）的HTTPS方式进行连接，对通信实体未采用合规的方式进行身份鉴别，存在非法设备或非授权人员接入网络的风险。

通信数据完整性：通过采用国际算法（算法）的HTTPS方式进行连接，未采用合规的密码技术保证通信过程中数据的完整性，存在数据传输过程中被非授权篡改的风险。

通信过程中重要数据的机密性：通过采用国际算法（算法）的HTTPS方式进行连接，未采用合规的密码技术保证通信过程中重要数据的机密性，存在数据传输过程中被窃取的风险。

网络边界访问控制信息的完整性：未采用合规的密码技术保证通信过程中网络边界访问控制信息的完整性，存在数据传输过程中被非授权篡改的风险。

安全接入认证：本系统不涉及此需求，不纳入本次测评范围。

1. 系统业务服务区和数据灾备区之间的专线通信信道

身份鉴别：目前系统业务服务区和数据灾备区之间的专线通信信道使用专线进行灾备数据传输，通信前未使用密码技术对通信实体双方进行验证， 存在非法通信实体接入网络的风险。

通信数据完整性：目前系统业务服务区和数据灾备区之间的专线通信信道使用专线进行灾备数据传输，未使用密码技术对灾备数据传输通道进行机密性和完整性保护，存在通信数据在信息系统外部被非授权篡改的风险。

通信过程中重要数据的机密性：目前系统业务服务区和数据灾备区之间的专线通信信道使用专线进行灾备数据传输，未采用合规的密码技术保证通信过程中重要数据的机密性，存在数据传输过程中被窃取的风险。

网络边界访问控制信息的完整性：未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护，存在非法设备从外部接入内部网络，或网络边界被破坏。

安全接入认证：本系统不涉及此需求，不纳入本次测评范围。

1. 公众用户移动端 APP与业务系统之间的通信信道

身份鉴别：目前互联网系统移动端 APP的通信信道使用HTTP协议建立数据传输通道，通信前未使用密码技术对通信实体双方进行验证， 存在非法通信实体接入网络的风险。

通信数据完整性：目前互联网系统移动端 APP的通信信道使用HTTP协议建立数据传输通道，未使用密码技术保证通信过程中数据的完整性，存在数据传输过程中被非授权篡改的风险。

通信过程中重要数据的机密性：目前互联网系统移动端 APP的通信信道使用HTTP协议建立数据传输通道，未采用密码技术保证通信过程中重要数据的机密性，存在数据传输过程中被窃取的风险。

网络边界访问控制信息的完整性：未使用密码技术对该条信道的网络边界访问控制信息进行完整性保护，存在非法设备从外部接入内部网络，或网络边界被破坏。

安全接入认证：本系统不涉及此需求，不纳入本次测评范围。

1. 普洱公积金综合服务平台与业务系统之间的通信信道

普洱公积金综合服务平台与业务系统之间的通信信道不涉及敏感数据的传输，故本次密码应用建设不进行改造。

网络环境需求分析

1. 内部用户PC浏览器与业务系统之间的通信信道

身份鉴别：通过部署合规的SSL VPN产品，建立单向的商密SSL传输通道，对通信实体进行身份鉴别，保证通信实体身份的真实性；

通信过程中数据的完整性：通过部署合规的SSL VPN产品，建立商密SSL传输通道，通过SSL VPN技术对通信数据进行完整性保护；

通信过程中重要数据的机密性：通过部署合规的SSL VPN产品，建立商密SSL传输通道，通过SSL VPN技术对通信过程中的重要数据进行机密性保护；

网络边界访问控制信息做完整性：通过部署合规的SSL VPN产品，建立商密SSL传输通道，通过SSL VPN技术对防火墙的访问控制列表、边界路由的访问控制列表等网络边界访问控制信息进行完整性保护；

安全接入认证：本系统不涉及此需求，故不做特殊改造。

1. 系统业务服务区和数据灾备区之间的专线通信信道

身份鉴别：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等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；

通信过程中数据的完整性：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制对通信数据进行完整性保护；

通信过程中重要数据的机密性：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于密码算法的解密功能实现通信过程中重要数据的机密性保护；

网络边界访问控制信息做完整性：通过部署合规的IPSec VPN产品，使用IPsec VPN建立安全传输通信信道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对IPsec VPN中的访问控制列表进行完整性保护。

安全接入认证：本系统不涉及此需求，故不做特殊改造。

1. 公众用户移动端 APP与业务系统之间的通信信道

身份鉴别：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等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；

通信过程中数据的完整性：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制对通信数据进行完整性保护；

通信过程中重要数据的机密性：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于密码算法的解密功能实现通信过程中重要数据的机密性保护；

网络边界访问控制信息做完整性：通过部署合规的SSL VPN产品，建立安全的移动端APP数据传输通道，基于对称密码算法或密码杂凑算法的消息鉴别码(MAC)机制、基于公钥密码算法的数字签名机制等密码技术对SSL VPN安全网关、防火墙、边界路由中的访问控制列表进行完整性保护；

安全接入认证：本系统不涉及此需求，故不做特殊改造。

3.1.3设备环境

设备环境风险分析

身份鉴别：本系统现阶段针对其上各设备均采用用户名+口令方式登录，未采用密码技术对通信实体进行身份鉴别，无法保证登录人员身份的真实性。

远程通道管理安全：本系统现阶段通过堡垒机进行各设备的远程管理，未采用合规的密码技术实现登录堡垒机的远程通道以及由堡垒机登录到各设备的通道安全。

系统资源访问控制信息完整性：本系统内各设备未采用密码技术保证系统资源访问控制信息的完整性，存在系统资源访问控制信息被非授权篡改的风险。

重要信息资源安全标记完整性：无重要信息资源安全标记。

日志记录完整性：本系统内各设备未采用密码技术保证日志记录的完整性，存在日志记录被非授权篡改的风险。

重要可执行程序完整性、重要可执行程序来源真实性：本系统内各设备未采用密码技术保证重要可执行程序完整性，无法保证重要可执行程序来源的真实性。

设备环境需求分析

本系统在设备和计算安全层面的测评对象共分为三类，分别为堡垒机、通用设备、密码设备。其中，通用设备包括：应用服务器和数据库服务器以及数据库管理系统；密码设备包括【服务器密码机、签名验签服务器、国密安全密码应用中间件、SSL VPN安全网关、密钥管理系统】。上述各产品均由堡垒机进行统一运维。根据上述场景总结出的三类测评对象有以下密码应用需求。

1、堡垒机

1. 身份鉴别：采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性。

{在密码基础设施区部署堡垒机，给运维人员配发已通过商用密码产品检测认证的USBKey（内存有合规的国密数字证书），首先通过SSL VPN安全网关接入内网，再登录堡垒机进行设备的运维管理，SSL VPN安全网关的身份鉴别措施可有效缓解运维人员登录堡垒机的身份鉴别风险，因此不对堡垒机进行改造。（不改造堡垒机）}

1. 远程管理通道安全：采用密码技术建立安全的信息传输通道，实现对远程管理人员的身份鉴别，以及传输数据的机密性和完整性保护。

{在网络边界处部署已通过商用密码产品认证的SSL VPN安全网关登录堡垒机，先通过国密SSL协议建立运维人员到内网的安全传输通道，再使用堡垒机自签的证书，通过非国密HTTPS协议建立运维人员到堡垒机的安全传输通道。（不改造堡垒机）}

1. 系统资源访问控制信息完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等进行完整性保护。
2. 重要信息资源安全标记完整性：设备不涉及重要信息资源安全标记，此项不适用。
3. 日志记录完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的日志记录进行完整性保护。

{由于堡垒机不支持日志记录调出，本次项目暂不考虑对堡垒机的日志记录完整性进行密码应用建设。（不改造）}

1. 重要可执行程序完整性、重要可执行程序来源真实性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的重要可执行程序进行完整性保护并实现其来源的真实性保护。

{由于堡垒机技术上无法实现，本次项目暂不考虑对堡垒机重要可执行程序完整性和重要可执行程序来源真实性进行密码应用建设。（不改造）}

2、通用设备

1. 身份鉴别：采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性。

{使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机利用用户名+口令对通用类产品进行运维过程中的身份鉴别。（不改造堡垒机）}

1. 远程管理通道安全：采用密码技术建立安全的信息传输通道，实现对远程管理人员的身份鉴别，以及传输数据的机密性和完整性保护。

{使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机，由堡垒机使用无高风险的SSH2协议对通用设备进行运维的过程中远程管理通道安全的保护。（堡垒机不改造）}

1. 系统资源访问控制信息完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对设备操作系统的系统权限访问控制信息、系统文件目录的访问控制信息、数据库中的数据访问控制信息、堡垒机等第三方运维系统中的权限访问控制信息等进行完整性保护。
2. 重要信息资源安全标记完整性：设备不涉及重要信息资源安全标记，此项不适用。
3. 日志记录完整性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的日志记录进行完整性保护。

{需部署已通过商用密码产品检测认证的服务器密码机保证应用服务器、数据库服务器以及数据库管理系统的日志记录的完整性，防止其被篡改。}

1. 重要可执行程序完整性、重要可执行程序来源真实性：采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对上述设备中的重要可执行程序进行完整性保护并实现其来源的真实性保护。

{需部署已通过商用密码产品检测认证的签名验签服务器保证应用服务器、数据库服务器以及数据库管理系统的重要可执行程序完整性以及来源的真实性。}

3、密码设备

1. 身份鉴别：需部署采用已通过商用密码产品检测认证的USBKey（内存有合规的国密数字证书）登录，并调用已通过商用密码产品检测认证的签名验签服务器进行验签，对运维人员进行身份鉴别，防止非授权人员登录。

{设备登录人员使用Ukey登录，采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对设备运维管理人员等登录设备的用户进行身份鉴别，保护登录设备用户的身份真实性}

1. 远程管理通道安全：{密码设备通过堡垒机运维，堡垒机与密码设备之间需采用国密技术或密码技术构建安全的远程管理通道。}

{设备本地运维，不涉及远程管理通道，该指标作为不适用项处理。}

{使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机，由堡垒机使用无高风险的HTTPS协议对各密码设备进行运维的过程中的远程管理通道安全的保护。（堡垒机不改造）}

1. 系统资源访问控制信息完整性：上述密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备访问控制信息的保护。
2. 重要信息资源安全标记完整性：上述密码设备不涉及重要信息资源安全标记，该指标不适用。
3. 日志记录完整性：上述密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备日志信息的保护。
4. 重要可执行程序完整性、重要可执行程序来源真实性：上述密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对重要可执行程序完整性、真实性的保护。

3.2业务应用

业务应用风险分析

身份鉴别：通过PC浏览器访问业务系统的内部员工，目前采用用户名+口令的方式登录业务系统，未采用合规的密码技术对登录用户进行身份鉴别，存在非授权人员登录的风险。

访问控制信息完整性：系统中未采用密码技术对访问控制信息进行完整性保护，存在访问控制信息被篡改的风险。

重要信息资源安全标记完整性：本系统无重要信息资源安全标记，此项不适用。

重要数据存储机密性：系统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，存在重要数据在存储过程中被窃取的风险。

重要数据存储完整性：系统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性。存在重要数据在存储过程中被非授权篡改的风险。

重要数据传输机密性：系统未采用合规的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，存在重要数据在传输过程中被窃取的风险。

重要数据传输完整性：系统未采用合规的密码技术保证信息系统应用的重要数据在传输过程中的完整性，存在重要数据在传输过程中被非授权篡改的风险。

不可否认性：本系统不涉及法律责任认定的应用场景，在本次密码应用改造及测评时，作不适用项处理。

{系统未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。}

业务应用需求分析

身份鉴别：通过PC浏览器访问业务系统的内部员工，应采用合规的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，防止非授权人员登录。

{采用动态口令机制、基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，在XXXX用户登录系统时对登录用户进行身份鉴别。（选择实际使用到的密码技术）}{XX{用户类型，如普通用户}{通过XX系统（第三方系统名称，如省统一身份认证平台）登录，}使用{账号口令+手机短信验证码/扫码/刷脸}方式登录业务系统，降低了应用和数据安全层面用户身份鉴别的风险。}

访问控制信息完整性：应采用密码技术对访问控制信息进行完整性保护，防止访问控制信息被篡改。

{采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对应用系统的权限、标签等能够决定系统应用访问控制的措施等信息进行完整性保护。}

重要信息资源安全标记完整性：本系统不涉及重要信息资源安全标记，故不做特殊改造。

重要数据传输机密性：应通过调用合规的密码设备或产品，对业务应用的重要数据进行传输机密性保护，实现重要数据防窃取保护。

{采用密码技术的加解密功能，对系统重要数据进行传输过程中的机密性保护。}（只有在应用层面传输做了数字信封，才能描述重要数据进行了应用层面的传输机密性保护）

{依赖网络层构建的安全通道缓解。}（数据传输不进行改造，通过网络层缓解）

重要数据传输完整性：应通过调用合规的密码设备或产品，对业务应用的重要数据进行传输完整性保护，防止被非授权篡改。

{采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术对信息系统应用中重要数据进行传输过程中的完整性保护。}（只有在应用层面传输做了数据源的完整性保护，才能描述重要数据进行了应用层面的传输完整性保护）

{依赖网络层构建的安全通道缓解。}（数据传输不进行改造，通过网络层缓解）

重要数据存储机密性：应通过调用合规密码设备或产品，对业务应用的重要数据进行存储机密性保护，实现重要数据防窃取保护。

{采用密码技术的加解密功能，对系统中重要数据进行存储过程中的机密性保护。}

重要数据存储完整性：应通过调用合规的密码设备或产品，对业务应用的重要数据进行存储完整性保护，实现重要数据防篡改保护。

{采用密码技术的加解密功能，对系统中重要数据进行存储过程中的机密性保护。采用基于对称密码算法或密码杂凑算法的消息鉴别码（MAC）机制、基于公钥密码算法的数字签名机制等密码技术，对系统的重要业务日志做完整性保护}

不可否认性：本系统不涉及法律责任认定的应用场景，在本次密码应用改造及测评时，作不适用项处理。

{采用基于公钥密码算法的数字签名机制等密码技术，对XXX{示例：系统用户的事项申请行为、业务办理审批行为}等关键行为进行签名，实现数据原发行为和数据接收行为的不可否认性。}

3.3安全管理

安全管理风险分析

单位根据等保2.0管理要求，目前虽然已经制定了通用的《某部信息 安全管理制度汇编 》，但该安全管理制度汇编内容仅涉及安全管理制度、安全管理机构、人员安全管理、系统建设管理、系统运维管理等5个方面的安全管理要求。未对密码应用的管理制度、人员管理、建设运行和应急处置等方面制定专用的密码应用管理制度。

未依据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中的安全管理要求，制定密码相关管理制度，不利于在本系统中落实密码相关国家政策要求，不利于发挥密码在信息系统安全中的基础支撑作用。

安全管理需求分析

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》，从管理制度、人员管理、建设运行、应急处置等4个方面制定并建设密码应用管理保障体系。需制定本系统的密码应用方案，并委托密评机构对密码应用方案进行评估，评估通过后按照本方案完成系统密码应用建设，委托合规的第三方测评机构依据密码应用方案对本系统进行密码应用安全性评估，评估通过后上线运行。

4 安全目标及设计原则

4.1安全目标

围绕GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中关于信息系统在系统规划阶段的密码应用要求，综合考虑物理和环境、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GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中三级指标要求，确保信息系统可顺利通过密码应用安全性评估，提升XXX系统在密码应用安全性，确保密码应用的正确性、合规性。

4.2设计原则与依据

**1.整体性原则。**按照GB/T 39786对信息系统密码应用的基本要求,以及信息系统的安全需求、责任单位的密码应用规划和密码管理需求,进行顶层设计。

**2.科学性原则。**参考信息系统的密码需求、管理需求和整体规划,合理整合和部署密码资源,切实解决应用中的安全问题。

**3.完备性原则。**依据法律、法规、标准等关于密码使用的要求,设计满足信息系统安全需求的密码应用方案。

**4.可行性原则。**密码应用方案切合实际,便于实现,能作为信息系统密码应用建设、验收和密码应用安全性评估的依据。

**5.合规性原则。**密码应用方案中使用的密码算法遵循国家有关法律法规的要求;使用的密码技术遵循国家及行业相关标准:涉及国家安全、国计民生、社会公共利益的信息系统,其使用的密码产品和服务经商用密码认证机构认证合格。

**主要依据**

* + - GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》
    - GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》
    - GB/T 37092-2018 《信息安全技术密码模块安全要求》
    - GM/T 0071-2019《电子文件密码应用指南》
    - GB/T 33482-2016《党政机关电子公文系统建设规范》
    - GM/T 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
    - GB/T 36968-2018《信息安全技术 IPSec VPN技术规范》
    - GM/T 0024-2014《SSL VPN 技术规范》
    - GM/T 0025-2014《SSL VPN 网关产品规范》
    - GM/T 0026-2014《安全认证网关产品规范》
    - GM/T 0030-2014《服务器密码机技术规范》
    - GM/T 0031-2014《安全电子签章密码技术规范》
    - GM/T 0027-2014《智能密码钥匙技术规范》
    - GM/T 0014-2012《证书认证系统密码协议规范》
    - GM/T 0033-2014《时间戳接口规范》
    - GM/T 0029-2014《签名验签服务器技术规范》

5.密码应用设计

5.1密码应用技术框架

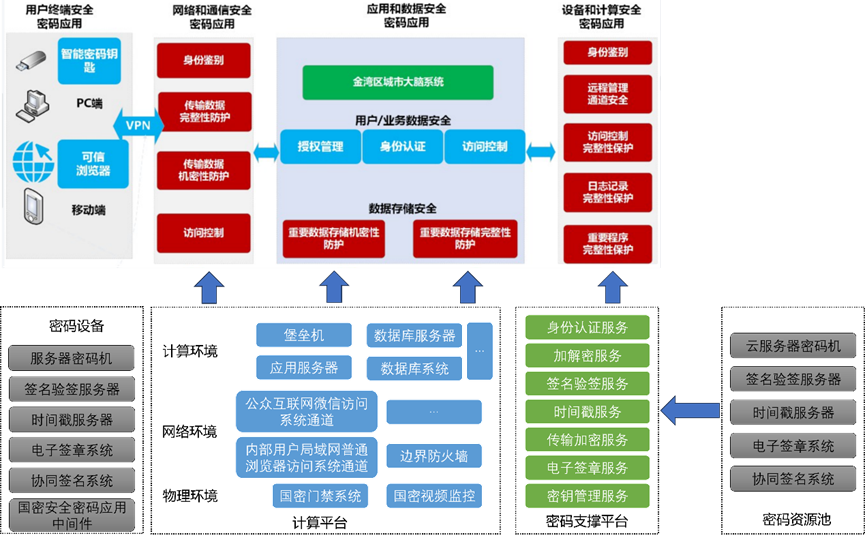
**GB/T 43207-2023《信息安全技术信息系统密码应用设计指南》要求此章节内容：包括密码应用技术框架图及框架说明。密码应用技术框架包括计算平台、密码支撑平台和业务应用密码应用架构等,综合描述各平台、系统之间的关系,清晰展示密码应用整体技术框架。示例写法如下：**

普洱公积金综合服务平台密码应用技术框架如下图2所示。

下图二选一



**图2密码应用技术框架（非云）**

****

**图2密码应用技术框架（云）**

密码产品主要实现说明如下：

普洱公积金综合服务平台的密码应用架构分为密码资源池、密码支撑平台、计算平台、密码应用层，密码应用层包括用户终端安全密码应用、网络接入网络和通信安全密码应用、业务安全密码应用和数据安全密码应用、平台管理安全密码应用设备和计算安全密码应用四部分。

**1、密码支撑平台**

密码支撑平台为云密码服务平台提供基础的密码运算资源。为业务应用提供身份认证、数据加密、操作不可否认、数字证书管理等密码应用所需基础服务。当单位用户通过PC端连接SSL VPN，浏览器访问系统时需通过智能密码钥匙USBKey进行身份验证，以避免其用户名/口令遭到截获、假冒或重用，导致业务应用系统被入侵，将造成用户身份信息泄露、业务系统其他信息泄露或伪造业务指令风险。数据在传输时需通过服务器密码机、国密安全密码应用中间件、进行加密传输，保证用户信息不被窃取偷听篡改等，以保障传输过程的机密性与完整性。

**2、密码资源池**

基于各密码产品构建的密码基础服务层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。

密码资源池整合服务器密码机、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，对外统一提供密码服务、集约化建设，密码服务可弹性扩展。

以下密码产品均满足GB/T 37092-2018《信息安全技术 密码模块安全要求》或GM/T 0028-2014《密码模块安全技术要求》密码模块二级及以上。

1)服务器密码机：遵循GM/T 0030-2014《服务器密码机技术规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GM/T 0028-2014《密码模块安全技术要求》和GM/T 0059-2018《服务器密码机检测规范》；支持SM1、SM2、SM3、SM4等国产密码算法；支持RSA、AES、3DES、MD5、SHA等国际算法；具有商用密码产品认证证书；支持数据加密/解密、数字签名/验签、消息鉴别码的产生/验证、数字信封、密钥协商等类型的密码运算，并且支持多任务并发访问；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；支持100对SM2非对称密钥、100对RSA非对称密钥、200个对称密钥，并使用管理密钥加密存储；采用双路国家密码管理局批准的物理噪声源随机数芯片；支持管理员、操作员角色，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；同时支持SDF、JCE、PKCS11接口，具有良好的通用性。

2)签名验签服务器：遵循GM/T 0028-2014《密码模块安全技术要求》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GB/T 38629-2020《信息安全技术 签名验签服务器技术规范》、GM/T 0029-2014《签名验签服务器技术规范》和GM/T 0060-2018《签名验签服务器检测规范》；支持SM1、SM2、SM3、SM4等国产密码算法；支持RSA,3DES,AES,SHA等常见国际算法；具有商用密码产品认证证书；支持与CA连接，提供证书管理功能，支持CA、CRL、OCSP等多种方式证书有效性验证；支持基于SM2、RSA算法数字证书的数字签名、验证签名等服务，以保证业务信息的真实性、完整性和不可否认，提供对PKCS#1、PKCS#7 Attach、PKCS#7 Detach、XML等电子数据的数字签名/验签功能，提供对消息、文件等多种格式的运算方式；支持基于SM2、RSA密码算法的数字信封功能，支持PKCS#7标准各种格式的数字信封封装和解封；由签名验签服务器产生应用实体的签名密钥对和证书请求，支持通过管理界面导入应用实体的签名证书、加密证书和加密密钥对；设备内可存储至少200个对称密钥以及100对非对称密钥，并且支持加密存储或微电保护存储；具备完善的身份鉴别机制，通过智能密码钥匙与口令相结合的方式实现管理员身份的鉴别；通过连接白名单的支持，实现了签名验签服务器对应用服务器的授权认证。

3)国密安全密码应用中间件：信息系统与密码应用系统及密码设备之间的重要中间件；提供数据加解密、签名验签、数字信封、摘要计算、随机数等接口服务能力；支持对接不同厂商的各类异构密码设备（包括服务器密码机、签名验签服务器、时间戳服务器、云密码机等），并将密码设备进行会话级别（Session）的细粒度管理与调度；内置基础证书与密钥管理能力，可对接具有商密产品认证资质的CA、密钥管理系统，以提供证书与密钥的全生命周期管理能力；内置密码机软件模拟器，可方便开发人员进行应用无密码设备开发集成与调试，可与硬件密码设备无缝切换；可以支持多应用系统接入，并通过数字证书对应用系统进行访问控制；为应用开发提供支持包括C/C++、Java、Go、PHP、.Net、Shell等语言的密码服务接口调用。

4)国密数字证书：由受信任的数字证书颁发机构（CA），在验证身份信息（包括域名、主机名、服务器名、申请者身份、机构身份等）后颁发。支持SM2等国产密码算法。

5)智能密码钥匙：遵循GM/T 0027-2014《智能密码钥匙技术规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GB/T 35291-2017《信息安全技术 智能密码钥匙应用接口规范》、GM/T 0028-2014《密码模块安全技术要求》和GM/T 0048-2016《智能密码钥匙密码检测规范》；支持国产密码算法；实现密码运算、密钥管理功能的终端密码设备，提供USB接口；支持数据加解密、消息鉴别码等功能；至少支持三种密钥，包括设备认证密钥、用户密钥、会话密钥，具有对用户密钥和会话密钥的产生、存储、使用、导入、导出、协商等功能；能够至少保存2对RSA密钥对、2对SM2密钥对和2个对称密钥（设备认证密钥和会话密钥）；随机数由多路硬件噪声源产生；证书管理：支持数字证书的读写、枚举、删除，可作为数字证书的安全载体。

6)SSL VPN安全网关：遵循GM/T 0025-2014《SSL VPN 网关产品规范》、GB/T 37092-2018《信息安全技术 密码模块安全要求》、GM/T 0028-2014《密码模块安全技术要求》；支持SM2、SM3、SM4国产密码算法；具有商用密码产品认证证书；基于 SSL/TLS 协议，在通信网络中构建安全通道；随机数由多路硬件噪声源产生；提供密钥交换功能，通过协商产生工作密钥；提供符合国际和国密标准SSL的VPN通道防护，有安全报文传输功能，支持抗重放攻击，保证数据的安全传输；通过数字证书的方式对实体鉴别，保证鉴别信息的完整性和有效性；具有细粒度的访问控制功能，基于用户或用户组对资源进行有效控制，并能根据访问时间进行控制；根据时间周期或报文流量进行工作密钥更新；能够对用户对系统的访问进行详细记录，记录信息包括：时间、用户IP、用户证书信息、访问资源、上传流量、下载流量、访问结果、错误原因；用户访问HTTP应用时，系统在完成相应的身份鉴别后，把验证结果、用户基本信息插入到HTTP请求中传送给后台的应用系统，应用系统通过标准的HTTP操作即可获取信息，并基于该信息作相应的访问控制以及进行相应的业务审计；客户端在连接服务端时，根据服务端下发的客户端安全策略检查用户操作系统的安全性。

7)可信浏览器：支持SM2、SM3、SM4国密算法；具有商用密码产品认证证书；支持国密SSL双向协议；支持最新TLCP标准；支持沙箱机制、浏览器内核隔离域、跨域安全隔离、站点安全隔离防护、可信证书校验等功能；支持本地用户数据加密，防止用户保存的密码被明文导出；支持国密网站、国密应用自动识别及国密标识展现，针对国密网站优先通过国密协议访问，单向SSL连接性能不低于200次/秒；可信浏览器管控中心支持证书的统一导入和下发，证书下发支持RSA国际证书和国内商密证书。

8)协同签名系统：支持SM2、SM3、SM4等国产密码算法；具有商用密码产品认证证书； SM2私钥使用密钥分割技术生成，从生成到运算整个过程中不出现完整的SM2私钥，保障了私钥的安全；对终端移动终端进行管理，包括设备的查看、挂起、停用；支持对接第三方CA系统：导入CA获取的证书和私钥数据，并解析传入的证书相关信息；支持数据签名/验签，数字信封封装/解析等类型的密码运算；支持管理员、审计员、操作员角色：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。

5.2计算平台密码应用方案

5.2.1物理和环境安全

（云平台机房已密改通过密评描述）XXX{云平台名称}已通过密码应用安全性评估第三级评估且安全等级不低于云上应用，其密评报告中对XXX{云平台名称}的支撑能力进行了评估，XX机房作为被完全评估的支撑能力，能同时支撑云平台和云应用在物理和环境安全层面的密码应用安全，采用云平台密评对物理和环境安全的结论。

1、中心机房

1. 身份鉴别：物理和环境安全中的身份鉴别属于高风险项。但考虑到系统门禁系统现状和资金问题，可使用缓解措施：（1）机房部署电子门禁系统，通过指纹/人脸方式对进出机房的人员进行身份鉴别；（2）在机房出入口配备专人值守并进行登记，且采用视频监控系统进行实时监控，{视频监控系统由专人进行值守，定期检查门禁和视频监控系统的安全状态。}。采用上述方式，属于此高风险项的缓解措施，可酌情降低风险等级。
2. 电子门禁记录数据存储完整性：物理和环境安全中的电子门禁系统进出数据记录的存储完整性非高风险项。考虑到系统门禁系统现状和资金问题，可不使用国密电子门禁系统，不做改造。该项会达不到要求而不得分，但整体分值及格仍可通过密评。
3. 视频监控记录数据存储完整性：物理和环境安全中的电子监控系统进出电子监控音像记录数据的存储完整性非高风险项。考虑到电子监控系统现状和资金问题，可不使用国密电子监控系统，不做改造。该项会达不到要求而不得分，但整体分值及格仍可通过密评。

5.2.2网络和环境安全

1. **员工用户PC浏览器与业务系统之间的通信信道**

1)身份鉴别：部署已通过商用密码机构认证的SSL VPN安全网关，PC端部署VPN客户端，SSL VPN安全网关中配置由合规CA颁发的国密数字证书，基于SM2数字证书实现对服务端的证书进行身份鉴别，保证通信过程中通信实体身份鉴别的真实性。

2)通信数据完整性：部署符合已通过商用密码机构认证的SSL VPN安全网关，已通过商用密码机构认证，基于HMAC-SM3算法可保证通信过程中数据的完整性。

3)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SSL VPN安全网关，基于SM4算法可保证通信过程中重要数据的机密性。

4)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SSL VPN安全网关，SSL VPN安全网关具有细粒度的访问控制功能，基于用户或用户组对资源进行有效控制，并能根据访问时间进行控制，基于HMAC-SM3算法保证通信过程中访问控制信息的完整性。防火墙和边界路由未使用密码技术保护网络边界访问控制信息的完整性。

5)安全接入认证：该指标要求属性为“可”，不纳入本次测评范围。

**2、系统业务服务区和数据灾备区之间的专线通信信道**

1)身份鉴别：在系统在网络接入区和数据灾备区部署符合GB/T 36968-2018《信息安全技术 IPSec VPN技术规范》、GB/T 37092-2018 《信息安全技术密码模块安全要求》二级模块要求的IPSec VPN，使用IPsec VPN建立安全传输通信信道。建立IPsec协议安全传输通道时通过双向传递数字证书，在主模式下基于SM2算法实现通信实体的身份鉴别，数字证书由证书认证系统签发。

2)通信数据完整性：业务服务器IPsec VPN和数据灾备区IPsec VPN建立安全关联SA后，协商安全参数交换密钥，使用AH协议保证数据传输的完整性，AH协议使用SM3算法计算消息摘要，将摘要与数据一起加密。接收方使用相同的散列函数对收到的数据进行处理，并与收到的摘要进行比较，以验证数据的完整性。

3)通信过程中重要数据的机密性：业务服务器IPsec VPN和数据灾备区IPsec VPN建立安全关联SA后，协商安全参数交换密钥，使用ESP协议保证数据传输的完整性，协议使用SM4对称加密算法加密数据。接收方使用相同的密钥和加密算法对收到的数据进行解密，以恢复原始数据。

4)网络边界访问控制信息完整性：该条信道的网络边界访问控制信息主要为IPsec VPN的访问控制列表信息，VPN已符合GB/T 37092-2018 《信息安全技术密码模块安全要求》二级模块要求，可通过自身较高的安全防护能力，基于SM2算法数字签名技术实现访问控制列表的完整性校验。

5)安全接入认证：该指标要求属性为“可”，不纳入本次测评范围。

**3、公众用户移动端APP与业务系统之间的通信信道**

1)身份鉴别：在服务端部署非国密站点证书（不包含高风险算法）实现通信实体身份鉴别，数字证书由具备资质的机构签发。

2)通信数据完整性：通过移动端APP和服务端构建非国密HTTPS通道，基于无高风险密码算法的HMAC技术实现通信数据完整性保护。

3)通信过程中重要数据的机密性：通过移动端APP和服务端构建非国密HTTPS通道，使用基于无高风险的密码算法对通信数据进行加密，实现通信过程中重要数据的机密性的保护。

4)网络边界访问控制信息的完整性：防火墙和边界路由未使用密码技术保护网络边界访问控制信息的完整性。

5)安全接入认证：本系统不涉及。

4、系统与系统、机房与机房之间的通信信道：通过纯物理裸光纤进行数据传输，作为不适用项处理。

5.2.3设备和计算安全

1、堡垒机

1)身份鉴别：在密码基础设施区部署堡垒机，给运维人员配发已通过商用密码产品检测认证的USBKey（内存有合规的国密数字证书），首先通过SSL VPN安全网关接入网络，再登录堡垒机进行设备的运维管理，SSL VPN安全网关的身份鉴别措施可有效缓解运维人员登录堡垒机的身份鉴别风险，因此不对堡垒机进行改造。（不改造堡垒机）

{使用支持国密算法的堡垒机，堡垒机通过密码产品认证。设备登录人员使用ukey登录堡垒机，ukey内置SM2数字证书，采用基于SM2算法的数字签名机制保证堡垒机登录人员身份的真实性。（国密堡垒机）}

{管理区部署堡垒机，运维人员PC端配发USBKey（内有国密数字证书），配合签名验签服务器的签名验签服务对运维人员进行身份鉴别。（改造堡垒机）}

2)远程管理通道安全：在政务外网出口区部署已通过商用密码产品认证的SSL VPN安全网关登录堡垒机，先通过国密HTTPS协议建立运维人员到内网的安全传输通道，再使用堡垒机自签的证书，通过非国密HTTPS协议建立运维人员到堡垒机的安全传输通道。（不改造堡垒机）

{堡垒机的远程管理通道，基于不包含高风险密码算法的非国密HTTPS协议保证远程管理通道安全。}

3)系统资源访问控制信息完整性：由于堡垒机不支持系统资源访问控制信息调出，本次项目暂不考虑对堡垒机系统资源访问控制信息完整性进行密码应用建设。

4)重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。

5)日志记录完整性：由于堡垒机不支持日志记录调出，本次项目暂不考虑对堡垒机的日志记录完整性进行密码应用建设。

6)重要可执行程序完整性、重要可执行程序来源真实性：于堡垒机技术上无法实现，本次项目暂不考虑对堡垒机重要可执行程序完整性和重要可执行程序来源真实性进行密码应用建设。

2、通用设备

1. 身份鉴别：使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机利用用户名+口令对通用设备进行运维过程中的身份鉴别。（不改造堡垒机）

{本项目将不考虑对通用设备进行改造，相关设备虽使用账号口令登录，但均使用堡垒机进行统一管理，能够降低相关设备身份鉴别所面临的安全风险。（改造堡垒机/国密堡垒机）}

1. 远程管理通道安全：使用商用密码产品检测认证的USBKey（内存有合规的国密数字证书），通过SSL VPN安全网关接入网络，再登录堡垒机，由堡垒机使用无高风险的SSH2协议对通用设备进行运维的过程中远程管理通道安全的保护。（不改造堡垒机）

{堡垒机到通用服务器、数据库管理系统的链路，使用非高风险密码算法，基于SSH2.0或者RDP协议（Linux系统：SSH2.0；Windows系统：RDP），采用公私钥体系的RSA2048算法的数字证书、采用SHA256和AES算法保证远程管理通道安全。}

1. 系统资源访问控制信息完整性：因全球信息化历史原因，各通用设备系统内核技术上无法实现基于密码技术的访问控制，本次项目暂不考虑对此类通用设备系统资源访问控制信息完整性进行密码应用建设。
2. 重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。
3. 日志记录完整性：部署已通过商用密码产品检测认证的服务器密码机，使用HMAC-SM3技术实现对通用设备的日志记录信息进行完整性保护。

{由于各类服务器之间协调难度大，密码改造成本高，同时设备部署在机房，机房具有完善的管理机制；且设备只由专人管理，未授权人员无权使用，通过严格的安全措施，保障了设备的安全运行。因此本项目暂不采用密码技术对上述设备的日志记录进行完整性保护。（不改造）}

1. 重要可执行程序完整性、重要可执行程序来源真实性：通用设备暂无机制保护其重要可执行程序。

**3、密码设备**

1)身份鉴别：运维人员通过堡垒机使用USBKey（内有数字证书认证系统签发的国密SM2证书）登录到各密码设备，配合已通过商用密码产品检测认证的签名验签服务器，在登录时验证运维人员USBKey中的国密数字证书实现运维人员登录密码设备的身份鉴别。

2)远程管理通道安全：由堡垒机使用无高风险的HTTPS协议对各密码设备进行运维管理，从而搭建安全的远程管理通道，实现运维人员登录堡垒机，从而对密码设备进行运维的过程中的远程管理通道安全的保护。

{密码设备均是本地运维，不涉及远程管理通道，该指标作为不适用项处理。}

{密码设备的远程管理通道，采用公私钥体系的RSA2048算法的数字证书、采用SHA256和AES算法保证远程管理通道安全，且通过堡垒机进行统一运维管理。}

3)系统资源访问控制信息完整性：密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备访问控制信息的保护。

4)重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。

5)日志记录完整性：密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对设备日志记录的保护。

6)重要可执行程序完整性、重要可执行程序来源真实性：密码设备经商用密码认证机构认证合格，且满足密码模块第二级安全要求，通过产品自身安全机制实现对重要可执行程序完整性、真实性的保护。

5.3密码支撑平台方案

（密码设备方式）

密码支撑平台为承载在计算平台上的普洱公积金综合服务平台系统提供密码功能服务，选择采用经认证合格的云服务器密码机、服务器密码机、签名验签服务器、时间戳服务器，基于经认证合格的密码产品进行设计。

5.3.1 密码服务机构的确定、接入方式和服务策略

采用机构颁发的数字证书。

网络层的国际或国密算法的站点证书，采用外部生成证书索引，后导入网关内生成站点证书的方式。

应用层的个人数字证书采用智能密码钥匙进行承载，线下签发制作的方式。

设备层的设备数字证书采用SSL VPN/时间戳服务器进行承载，线下签发制作的方式。

5.3.2 支持的密码体制和密码算法

（密码设备方式）

支持对称密码体制和非对称密码体制，密码算法支持RSA、AES、SHA-256、SM2、SM3、SM4。

5.3.3 接口和功能遵循的标准

（密码设备方式）

|  |  |  |
| --- | --- | --- |
| 序号 | 产品 | 遵循标准 |
| 1 | 服务器密码机 | 1、GM/T 0030《服务器密码机技术规范》  2、GM/T 0018《密码设备应用接口规范》  3、GM/T 0028《密码模块安全技术要求》 |
| 2 | 云服务器密码机 | 1、GM/T 0104《云服务器密码机技术规范》  2、GM/T 0018《密码设备应用接口规范》  3、GM/T 0028《密码模块安全技术要求》 |
| 3 | 签名验签服务器 | 1、GM/T 0029《签名验签服务器技术规范》  2、GM/T 0018《密码设备应用接口规范》  3、GM/T 0028《密码模块安全技术要求》 |
| 4 | 时间戳服务器 | 1、GM/T 0033《时间戳接口规范》  2、GM/T 0018《密码设备应用接口规范》  3、GM/T 0028《密码模块安全技术要求》 |
| 5 | SSL VPN | 1、GM/T 0024《SSL VPN网关产品规范》  2、GM/T 0025《SSL VPN技术规范》  3、GM/T 0028《密码模块安全技术要求》 |
| 6 | 智能密码钥匙 | 1、GM/T 0027 智能密码钥匙技术规范  2、GB/T 35291信息安全技术 智能密码钥匙密码应用接口规范 |

5.3.4 提供的密码支撑方式

采购符合规定的密码设备/租用密码设备/租用密码服务/建设密码资源

5.3.5 提供的密码功能及接口

密码功能及接口如下：

|  |  |
| --- | --- |
| 序号 | 提供的密码功能及接口 |
| 1 | 密钥管理 |
| 2 | 加密解密 |
| 3 | 消息鉴别码产生和验证 |
| 4 | 随机数产生 |
| 5 | 数据签名/验证 |
| 6 | 计算MAC/验证MAC |
| 7 | 签名验签 |
| 8 | 时间戳生成/验证/解析 |

5.3.6 部署的位置和方式

（密码设备方式）

密码设备部署在XX机房，以密码软硬件的方式进行部署。

5.3.7 接入计算平台的方式

非独立部署，使用XXX云平台/XX网的计算资源和网络资源。

5.3.8 密钥管理方式，按责任主体的规划要求确定

（密码设备方式）

密钥由密码设备生成和管理，密码设备的责任主体为XXX局。

5.3.9 支撑平台的自身安全性，包括密钥安全、访问安全、管理安全和租户间的隔离安全等

（密码设备方式）

使用密码设备对密钥安全、访问安全、管理安全和租户间隔离安全等进行保护。

本系统租用XXX云平台提供的密码服务实现，密钥由XXX进行管理（选择上述第8点的某种方式），上述内容的设计由XXX云平台进行统一规划、设计和管理。

5.4业务应用密码应用方案

**业务应用保护的对象是信息系统中的所有应用及其重要数据,按照GB/T39786中应用和数据安全对应等级的密码应用基本要求和各业务系统实际需求,对需要保护的对象进行密码应用方案设计,具体内容如下:**

**a）按照信息系统的规划、责任主体的需求,现有或规划的密码功能提供模式,确定密码体制**

**b）梳理业务流程,根据流程安全需求,为关键环节设计密码保护机制;梳理业务数据,根据数据安全需求,为重要数据设计密码保护机制;**

**c）梳理业务对象(如文件、证照、票据、病历、采集的数据和控制指令等),根据安全需求,为其设计密码保护机制；**

**e）根据角色和访问控制,为其权限和访问策略等设计密码保护机制;**

**f）根据审计策略,为日志记录设计密码保护机制;**

**g）为角色分配密钥,明确密钥载体,设计系统的密钥管理策略:**

**h）使用加密功能的,需指明密码算法、加密模式、数据填充方式和密钥属性等;**

**i）使用签名功能的,需指明签名算法和签名机制(如签名内容、签名主体和签名位置等);**

**j）使用完整性保护功能的,需指明使用的算法和校验机制;**

**k）根据保护机制,修改被保护对象的数据结构,将上述内容添加到原数据结构中,使其成为带安全机制的数据结构;**

**l）实现保护机制用到的密码功能和用户登录用到的身份鉴别功能,由密码支撑平台提供,数据传输和数据存储安全,由计算平台负责,有单独需求(如互通且长期保存)或计算平台没有提供的,可设计信源加密机制。**

**根据确定的密码体制和密码应用方案,设计密钥管理策略,内容包括密钥的种类和用途、密钥的载体和保管方式、密钥的使用和更新,密钥的备份和恢复等,分别针对上述内容所涉及的人员、责任、介质材料和流程等设计管理机制。示例写法如下：**

1. 身份鉴别：业务系统对接中间件做集成改造，系统管理员和内部用户PC端使用Ukey登录，Ukey内置SM2数字证书，登录时，服务器产生随机数，客户端使用数字证书对服务器端产生的随机数进行签名，服务器端通过密码应用服务系统的接口服务调用签名验签服务器进行验签，基于SM2数字签名技术保证登录用户身份的真实性。

采用USBKey登录的流程图如下图所示：

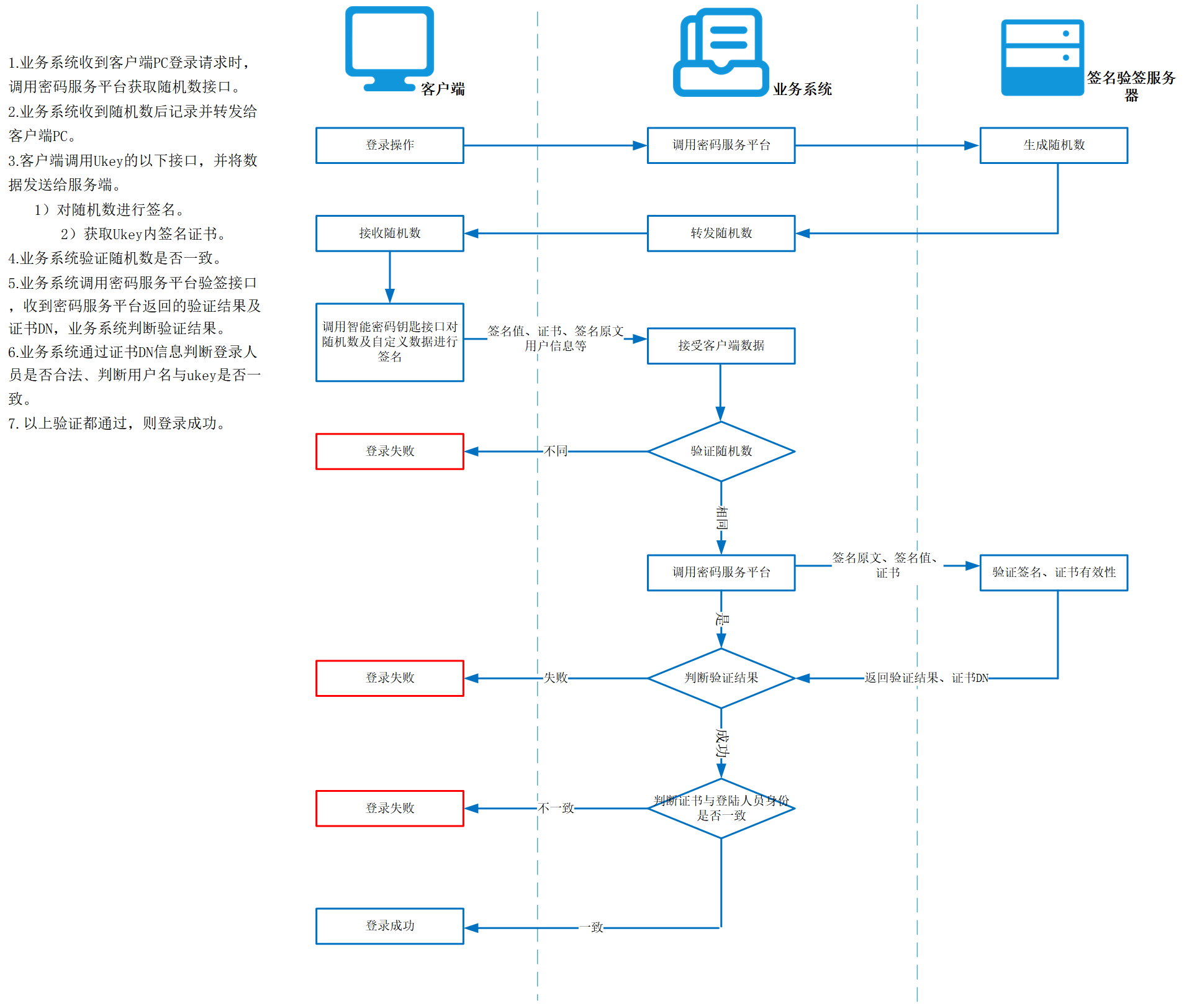


图 2 身份鉴别流程

1.业务系统收到客户端PC登录请求时，调用密码服务平台获取随机数接口。

2.业务系统收到随机数后记录并转发给客户端PC。

3.客户端调用Ukey的以下接口，并将数据发送给服务端。

1）对随机数进行签名。  2）获取Ukey内签名证书。

4.业务系统验证随机数是否一致。

5.业务系统调用密码服务平台验签接口，收到密码服务平台返回的验证结果及证书DN，业务系统判断验证结果。

6.业务系统通过证书DN信息判断登录人员是否合法、判断用户名与ukey是否一致。

7.以上验证都通过，则登录成功。

{XX{用户类型，如普通用户}{通过XX系统（第三方系统名称，如省统一身份认证平台）登录，使用{账号口令+手机短信验证码/扫码/刷脸}方式登录业务系统，降低了应用和数据安全层面用户身份鉴别的风险。（缓解措施）}

1. 访问控制信息完整性：部署具有商密资质的服务器密码机，业务系统通过中间件调用服务器密码机，使用HMAC-SM3算法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。
2. 重要信息资源安全标记完整性：本系统不涉及重要信息安全资源标记完整性。
3. 重要数据存储机密性：在密码基础设施区部署具有商密资质的服务器密码机和国密安全密码应用中间件，国密安全密码应用中间件采用插件模式，业务系统通过国密安全密码应用中间件调用服务器密码机，使用SM4算法对业务系统中的重要数据的存储进行机密性保护，防止其被非授权窃取。

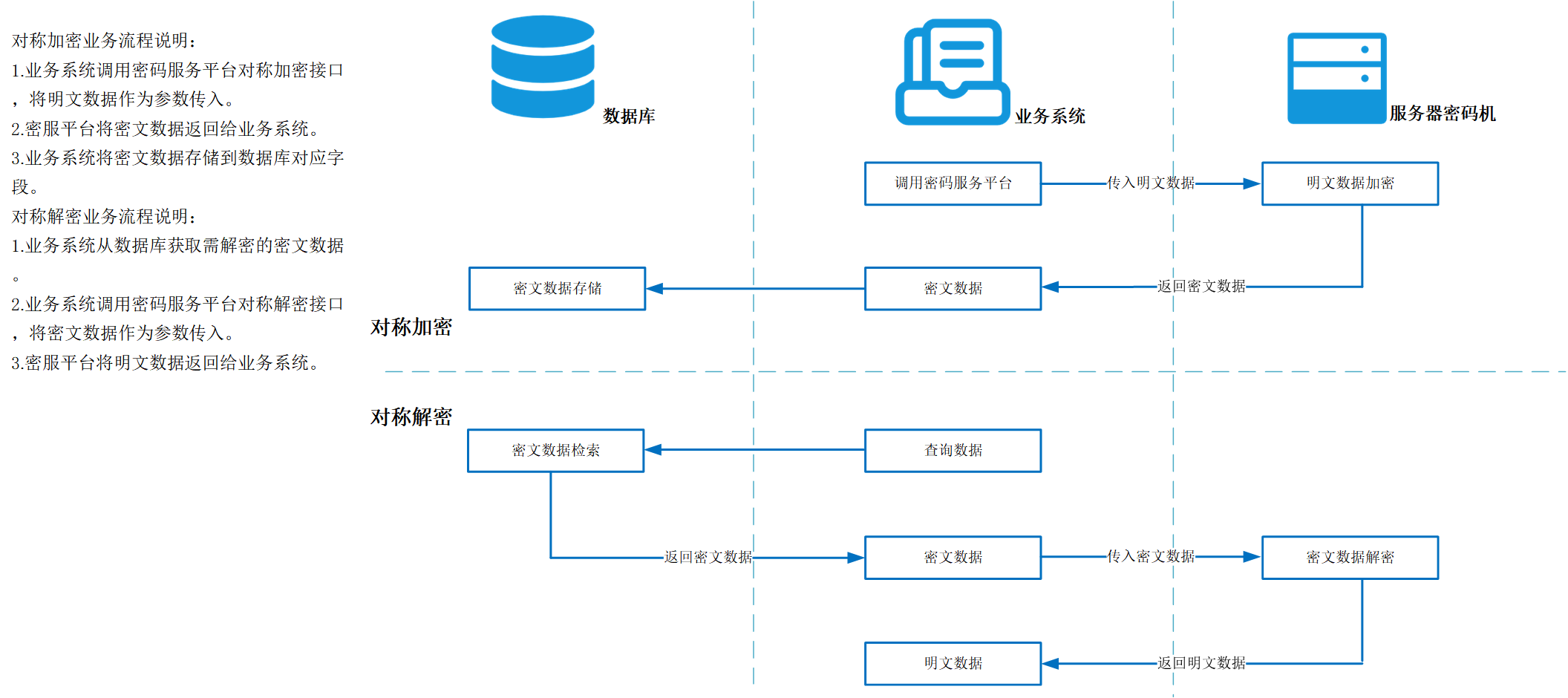


图 3 加密存储流程

对称加密业务流程说明：

1.业务系统调用密码服务平台对称加密接口，将明文数据作为参数传入。

2.密服平台将密文数据返回给业务系统。

3.业务系统将密文数据存储到数据库对应字段。

对称解密业务流程说明：

1.业务系统从数据库获取需解密的密文数据。

2.业务系统调用密码服务平台对称解密接口，将密文数据作为参数传入。

3.密服平台将明文数据返回给业务系统。

1. 重要数据存储完整性：在密码基础设施区部署具有商密资质的服务器密码机和国密安全密码应用中间件，国密安全密码应用中间件采用插件模式，业务系统通过国密安全密码应用中间件调用服务器密码机，使用HMAC-SM3对业务系统中的重要数据进行存储完整性保护，定期校验数据存储完整性，防止其被非授权篡改。

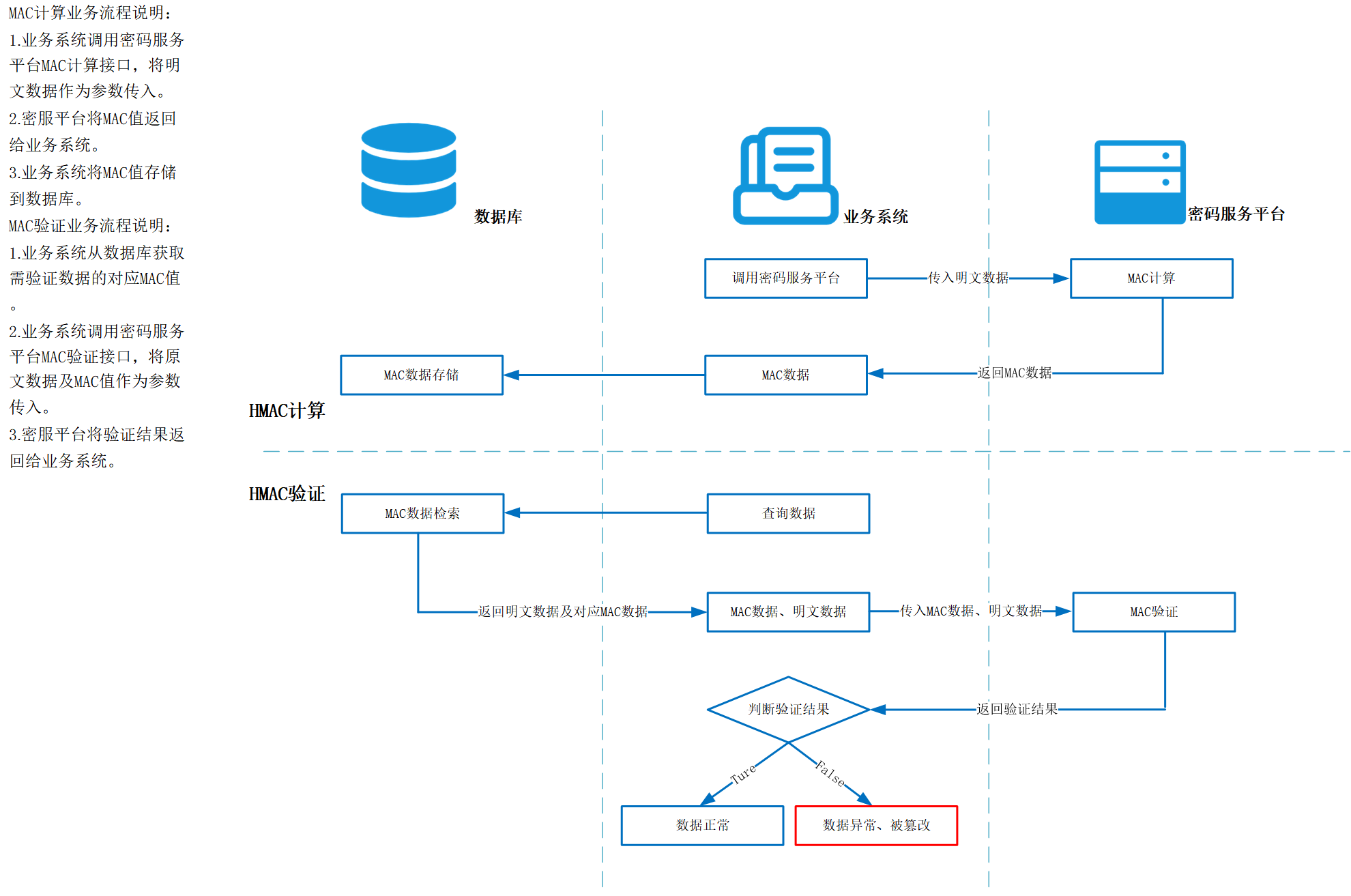


图 4 重要数据存储完整性保护

MAC计算业务流程说明：

1.业务系统调用密码服务平台MAC计算接口，将明文数据作为参数传入。

2.密服平台将MAC值返回给业务系统。

3.业务系统将MAC值存储到数据库。

MAC验证业务流程说明：

1.业务系统从数据库获取需验证数据的对应MAC值。

2.业务系统调用密码服务平台MAC验证接口，将原文数据及MAC值作为参数传入。

3.密服平台将验证结果返回给业务系统。

1. 重要数据传输机密性：部署已通过商用密码机构认证的SSL VPN安全网关，复用网络和通信层面搭建的国密SSL安全通信链路对重要数据传输进行机密性保护。
2. 重要数据传输完整性：部署已通过商用密码机构认证的SSL VPN安全网关，复用网络和通信层面搭建的国密SSL安全通信链路对重要数据传输进行完整性保护。
3. 不可否认性：本系统不涉及法律责任认定的应用场景，在本次密码应用改造及测评时，作不适用项处理。

{1.对于关键的操作行为，{操作者/应用系统}使用电子印章对关键操作行为和内容进行SM2算法/RSA算法的数字签名，签名内容为原数据的哈希值，签名主体为系统关键操作人员，签名位置为文件/网页，并由服务器端调用时间戳服务器加盖时间戳，把签名值、时间戳存到数据库。

在验证操作行为时，调用XX{密码设备名称，如签名验签服务器}对签名值进行验证，调用时间戳服务器校验时间戳，以此来实现关键操作的不可否认性。所使用的密码产品（UKey、时间戳服务器以及XX{密码设备名称，如签名验签服务器}）经商用密码认证机构认证合格，且满足密码模块第二级安全要求。

【病例、处方单、凭证等文件和文书，通过电子签章实现不可否认性】3.应用系统输出的{病例、处方单、凭证等文件和文书}），使用签发单位/签发人的电子印章，通过电子签章系统，对{病例、处方单、凭证等文件和文书}进行电子签章，签名算法为SM3+SM2，签名主体为公众用户，签名位置为文件或文书指定签名位置。

验证相关文件或文书时，通过调用安全电子签章系统进行验证，使用公钥验证电子签名值，实现关键操作的不可否认性。所使用的Ukey、安全电子签章系统经商用密码认证机构认证合格，其组件满足密码模块第二级安全要求，证书由合规的密码服务机构签发。}

**（添加流程）**

**密钥管理策略：**

1)密钥管理

| **序号** | **密钥名称** | **算法** | **用途** | **存储位置** |
| --- | --- | --- | --- | --- |
| 1 | 重要数据传输机密性保护密钥 | SM4 | 用于保护SSL通道中重要业务数据的传输机密性 | 临时协商，用完销毁 |
| 2 | 重要数据传输链路身份鉴别私钥 | SM2 | 用于建立链路时SSL客户端和服务端的身份鉴别 | 服务端在密码卡、客户端在UKEY |
| 3 | 重要数据传输链路身份鉴别公钥 | SM2 | 以证书形式使用，用于建立链路时SSL客户端和服务端的身份鉴别 | 服务端在密码卡、客户端在UKEY |
| 4 | 重要数据传输链路密钥协商私钥 | SM2 | 用于SSL客户端和服务端的密钥协商 | 服务端在密码卡、客户端在UKEY |
| 5 | 重要数据传输链路密钥协商公钥 | SM2 | 以证书形式使用，用于SSL客户端和服务端的密钥协商 | 服务端在密码卡、客户端在UKEY |
| 6 | 用户签名私钥 | SM2 | 系统管理员登录应用系统 | Ukey |
| 7 | 用户签名公钥 | SM2 | 以证书形式使用，用于系统管理员登录应用系统 | Ukey |
| 6 | 应用系统主密钥 | SM4 | 用于通过密钥分散技术，派生重要数据存储完整性保护密钥和重要数据存储机密性保护密钥 | 密码应用中间件数据库 |
| 7 | 应用系统主密钥保护密钥 | SM4 | 用于保护应用系统主密钥 | 服务器密码机 |
| 8 | 重要数据存储完整性保护密钥 | HMAC | 用于保护身份鉴别信息、重要业务数据、日志数据的存储完整性 | 临时分散，用完销毁 |
| 9 | 重要数据存储机密性保护密钥 | SM4 | 用于保护身份鉴别信息、重要业务数据的存储机密性 | 临时分散，用完销毁 |

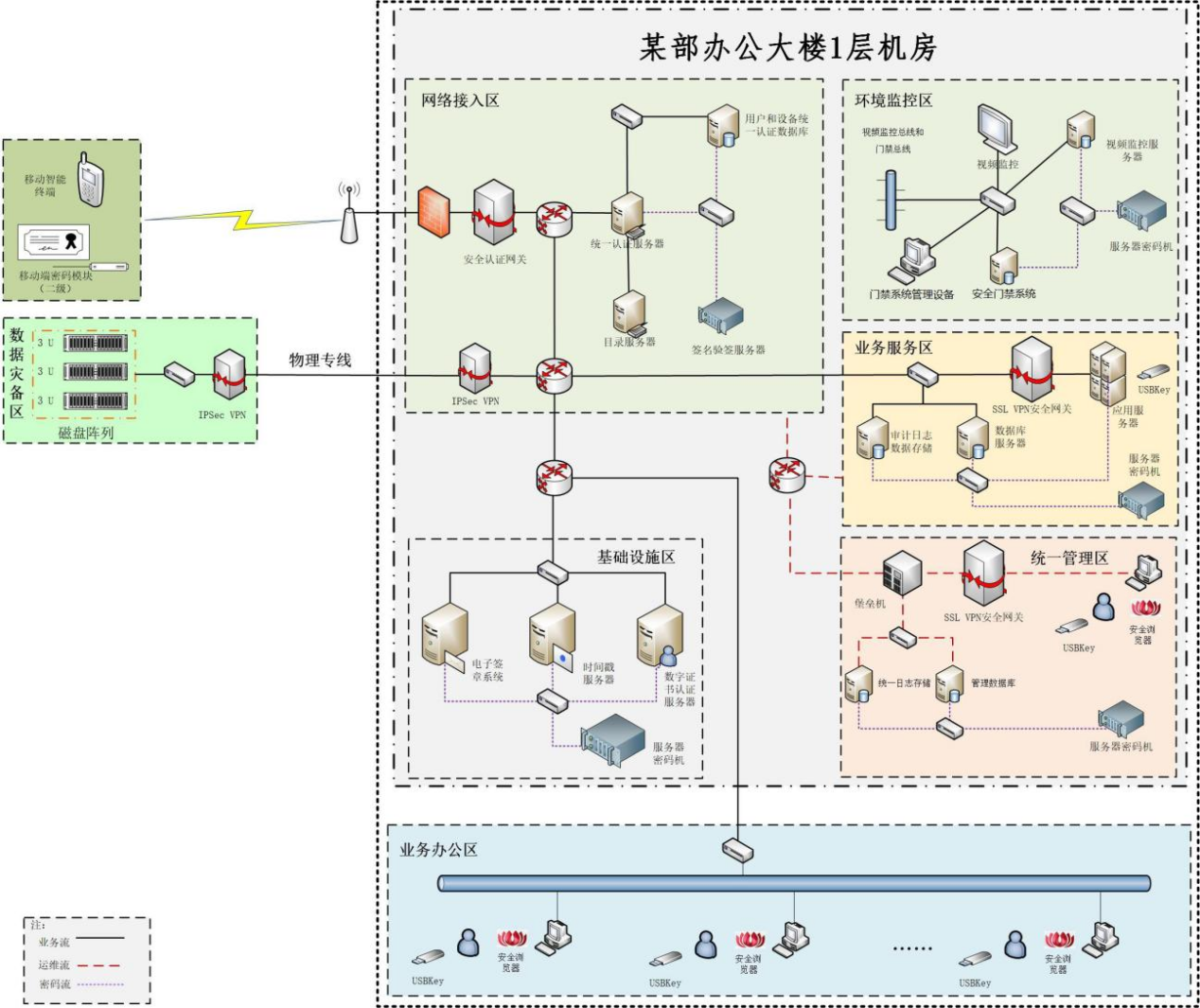
2) 密钥生命周期

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **生产** | **存储** | **分发** | **导入和导出** | **使用** | **备份和恢复** | **归档** | **销毁** |
| 1 | 重要数据传输机密性保护密钥 | SSL VPN客户端和服务端通过重要数据传密钥协商公私钥协商产生 | 临时协商、用完销毁 | 不涉及 | 不涉及 | VPN内部使用 | 不涉及 | 不涉及 | 临时协商、用完销毁 |
| 2 | 重要数据传输链路身份鉴别私钥 | VPN密码卡内部产生 | VPN密码卡内部存储 | 不涉及 | 不涉及 | VPN内部使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 3 | 重要数据传输链路身份鉴别公钥 | VPN密码卡内部产生 | VPN密码卡内部存储 | 不涉及 | 以公钥证书形式导入导出 | 以公钥证书形式使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 4 | 重要数据传输链路密钥协商私钥 | 由CA生产 | VPN密码卡内部存储 | 不涉及 | 不涉及 | VPN内部使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 5 | 重要数据传输链路密钥协商公钥 | 由CA生产 | VPN密码卡内部存储 | 不涉及 | 以公钥证书形式导入导出 | 以公钥证书形式使用 | VPN内部备份和恢复 | VPN内部归档 | VPN内部销毁 |
| 6 | 用户签名私钥 | 由ukey产生 | Ukey内部存储 | 不涉及 | 不涉及 | Ukey内部使用 | 不涉及 | 不涉及 | Ukey内部销毁 |
| 7 | 用户签名公钥 | 由ukey产生，由CA签发为公钥证书形式 | 以公钥证书形式存储 | 以公钥证书形式分发 | 以公钥证书导入导出 | 以公钥证书形式使用 | 不涉及、由CA备份和恢复 | 不涉及、 由CA归档 | 不涉及、 由CA销毁 |
| 8 | 应用系统主密钥 | 由密钥管理系统产生 | 密钥管理系统内部存储；  密码应用中间数据库密文存储； | 密钥管理系统使用密码应用中间平台根证书加密后分发至密码应用中间件；  密码应用中间将密文形式的应用系统主密钥分发至服务器密码机； | 不涉及 | 服务器密码机内部使用 | 密钥管理系统内部备份恢复 | 密钥管理系统内部归档 | 密钥管理系统内部销毁；密码应用中间件内部销毁 |
| 9 | 应用系统主密钥保护密钥 | 由服务器密码机内部产生 | 由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 | 服务器密码机内部备份恢复 | 不涉及 | 服务器密码机内部销毁 |
| 10 | 重要数据存储完整性保护密钥 | 由服务器密码机通过应用系统主密钥进行密钥分散内部产生 | 临时分散，用完销毁 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 临时分散，用完销毁 | 临时分散，用完销毁 | 临时分散，用完销毁 |
| 11 | 重要数据存储机密性保护密钥 | 由服务器密码机通过应用系统主密钥进行密钥分散内部产生 | 临时分散，用完销毁 | 不涉及 | 不涉及 | 服务器密码机内部使用 | 临时分散，用完销毁 | 临时分散，用完销毁 | 临时分散，用完销毁 |

5.5密码应用部署

**包括软硬件设备清单(软硬件设备均需包括已有的密码产品清单)、部署示意图及说明等,新增加的密码设备需要明确标识。示例写法如下：**

本系统部署和使用了【服务器密码机、签名验签服务器、SSL VPN安全网关、国密安全密码应用中间件、USBKey、IPSec VPN、电子签章系统、时间戳服务器】等密码产品，均具有商用密码产品认证证书，满足GB/T 37092-2018 《信息安全技术密码模块安全要求》标准二级模块要求。密码应用部署示意图如下：



**图3密码部署示意图**

1. 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安全网关之间，实现单向身份认证，确保授权用户身份的真实性。
2. 安全通道部署SSL VPN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安全网关之间的单向身份认证。运维人员通过安装SSL VPN客户端实现安全接入。
3. 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、密钥管理系统、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；密钥管理系统通过标准接口和不同密码设备对接，对外提供统一的密钥管理服务；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。

**密码软硬件产品：**

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，如下表所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 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 | 密码资源池 | 提供身份鉴别，保证关键业务信息的真实性、完整性和不可否认性 |  |  |
| 2 | 签名验签服务器 | 密码资源池 | 提供身份鉴别，保证关键业务信息的真实性、完整性和不可否认性 |  |  |
| 3 | 国密安全密码应用中间件 | 密码资源池 | 向下对接不同厂商的各类异构密码设备，向上提供统一的密码服务接口 |  |  |
| 4 | 密钥管理系统 | 密码资源池 | 通过标准接口和不同密码设备对接，对外提供统一的密钥管理服务 |  |  |
| 5 | 国密数字证书 | 智能密码钥匙 | 为系统提供基于密码技术的服务区分、标识、鉴别参与方身份/身份认证、电子签名/数据加密 |  |  |
| 6 | 智能密码钥匙 | 用户及运维人员PC端 | 用于PC端登录，实现登录人员的安全身份鉴别，防止非授权人员登录 |  |  |
| 7 | SSL VPN安全网关 | 网络接入区 | 基于国密SSL协议保证移动端、PC端与站点之间构建安全通道的设备 |  |  |
| 8 | IPSec VPN安全网关 | 网络接入区 | 为进行数据灾备的通信双方进行双向 身份鉴别， 对数据 备份传输通道进行 传输机密性、 完整性保护 |  |  |

6 安全管理方案

6.1管理制度

保障商用密码应用的合规性、正确性和有效性，除了技术，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》，分别从密码安全管理制度、人员管理、密钥管理、建设运行、密码软硬件及介质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。

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、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。

6.1 密码安全管理制度

为了加强密码设备管理工作，确保安全使用密码，根据《中华人民共和国密码法》、《商用密码管理条例》、GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》等国家有关法规规定，制定本制度。单位涉及密码管理、使用和运维等相关人员均需遵守本规定。

6.1.1 密码建设要求

1、信息系统密码建设应符合密码相关法律与行业相关政策要求进行建设。

2、统筹系统密码应用，应与业务系统统一设计，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。

3、信息系统规划阶段，依据相关标准，制定密码引用方案，组织专家进行评审，评审意见作为项目规划立项重要材料。通过专家审定后的方案应作为建设、验收和测评的重要依据。

4、对未及时开展密码建设的系统，应逐步完成密码建设的备案、整改、测评等工作。

5、密码建设产品应当采用符合国家密码管理部门核准的密码产品、许可的密码服务，产品应具备最新商用密码产品型号证书的产品。

6.1.2 密码运行要求

1、信息系统投入运行前，应经过密码测评机构进行安全性评估，评估通过方可投入正式运行。

2、信息系统投入运行后，本单位主管责任人应委托密码测评机构开展密码应用安全性评估，并根据评估意见进行整改；如若有重大安全隐患，应停止系统运行，制定整改方案，整改完成并通过后方可投入运行。

6.1.3 密码人员管理要求

1、结合系统分析、风险分析和安全需求分析的结果，明确密码安全管理人员。

2、结合系统建设具体现状明确本管理机构内密码管理人员组成与职能，明确管理责任，做到责任到部门、责任到人。

3、根据密码管理政策、数据安全保密政策，结合本组织实际情况，设立密钥管理员、密码安全审计员、密码操作员等关键安全岗位。

4、密钥管理员、密码安全审计员、密码操作员人员职责相互制约相互监督，关键设备的管理和使用账号不得多人共用。

5、建立人员考核制度，定期进行岗位人员考核，建立健全奖惩制度。

6、建立人员培训制度，对于涉及密码的操作和管理以及密钥管理人员进行专门培训。

7、建立关键岗位人员保密制度和调离制度，签订保密合同，承担保密义务。

6.1.4 密码使用责任要求

1、密码使用单位应当建立密码管理责任人，落实信息系统密码应用工作。

2、密码使用单位应严格遵循相关要求，使用密码技术完善系统的安全保护功能，因密码使用不当导致信息泄密、数据破坏的，追究相关单位密码管理部门和管理人员责任，并按要求整改。

3、本单位应当严格遵守相关保密制度，保管好个人数字证书，不得出借或使用他人证书登录信息系统平台。

4、个人数字证书介质一旦丢失，应立即进行挂失，并按规定流程到证书发放机构申请新的证书和介质。

6.1.5 密码设备维护规定

1、密码设备维护人员需经过培训，取得相关资质才能上岗，并需严格按照设备维护规范和使用说明开展维护工作。

2、密码设备应当按照要求定期完成设备巡检、升级和维保工作，至少每半年集中检查一次，密码设备操作必须经过授权，且不得接入互联网访问。

3、建立密码设备故障和应急保障机制，定期开展应急演练，确保设备发生故障时能及时上报、恢复。事件处理完成后及时向同级密码负责人报告事件发生情况和处理办法。

4、加强密码设备的日常监控，评估系统安全风险，及时进行扩容和升级。

6.2 人员管理

依据本单位《商用密码安全管理制度》设立本管理制度，主要用于对人员的相关合规性要求、培训、奖惩制度的说明和建立。

6.2.1 总章

密码人员应了解并遵守密码相关法律法规。

在岗密码人员应能够正确、合理使用密码产品。

6.2.2 第一章 密码人员岗位与职责

1、结合系统分析、风险分析和安全需求分析的结果，明确密码安全管理人员。

2、结合系统建设具体现状明确本管理机构内密码管理人员组成与职能，明确管理责任，做到责任到部门、责任到人。

3、根据密码管理政策、数据安全保密政策，结合本组织实际情况，设立密钥管理员、密码安全审计员、密码操作员等关键安全岗位，并制定规范边界任务。

1. 密码系统管理员职责

制定严格的规章制度并认真执行。建立完善的变更管理审核和批准制度，对任何可能影响系统正常运行的密码软硬件变更，包括更改设置、软硬件升级等，应及时登记报备。

1. 密钥管理员职责

负责对应用系统密钥的保管、监督、变更、撤销等具体操作，包括对密钥的生成、存储、分发、导入导出、使用、备份恢复、归档、销毁等全生命周期的管理。协助完成定期或不定期的专项辅导检查工作。

1. 密码安全审计员职责

密码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。

1. 密码操作员职责

认真执行密码安全相关制度；管理用户账户的密码，包括密码重置、设置和解锁；遵循密码策略，确保用户密码的复杂性和安全性；记录密码变更和重置的审计日志。协助完成定期或不定期的专项辅导检查工作。

6.2.3 第二章 密码人员培训规范

1、制定密码人员学习管理制度。制定密码人员学习、培训档案管理、培训考核等相关制度要求。

2、培训参加。定期参与省密码管理局开展的密码培训会议，使密码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。建立本单位内密码培训工作档案，记录包括培训范围、培训方式、培训内容、培训人数、培训时间和其他情况。

3、人员档案管理。建立针对密码管理人员建立员工培训档案，接收培训的具体情况和培训结果应详细记录备案，包括培训时间、培训地点、培训内容、培训目的以及培训效果。

4、培训档案管理。应对培训过程进行记录保存，培训资料应以纸质、电子文档、录音、录像等形式记录保存，并通过口令或专用加密软件加密保存至专用存储设备（如U盘、移动硬盘、NAS服务器等，纸质应单独文件柜）统一管理，培训档案留存时间应保存五年，五年后可销毁。

5、日常工作应用。针对密码人员的日常工作进行评估，针对培训填写“课程评估调查表”对省密码管理局是否具备工作改善计划或方案。

6.2.4 第三章 密码人员考核与奖惩

1、依托本单位人员绩效考核管理制度，制定密码人员考核管理办法。

2、针对测评机构、市密码管理局、省密码管理局、国家密码管理局的定期检查、抽查效果作为基本考核单元。对重大隐患、系统测评问题应及时上报处理、备案。

3、定期针对业务系统开展密码使用情况年度自查，并纳入责任单位相关人员考核。

4、在当年密码应用考核中被处理的，原则上取消当年评优评先资格。

5、在当年密码应用考核中表现突出的，依托本单位人员绩效考核管理制度酌情予以表彰、评优评先。

6.3 密钥管理

本单位依据《商用密码安全管理制度》设定对密钥管理的相关管理制度。管理内容包括对密钥的生成、存储、分发、导入、导出、使用、备份、恢复、归档、销毁等环节进行管理和策略制定的全过程。

6.3.1 密钥生成

本单位所使用的密钥生成使用的随机数均符合GM/T 0005要求，密钥均在符合GM/T 0028的密码模块中产生；密钥均在密码模块内部产生，不会以明文方式出现在密码模块之外；密码模块均具备检查和剔除弱密钥的能力。

6.3.2 密钥存储

本单位所使用的密钥均采用加密存储，并采取严格的安全防护措施，防止密钥被非法获取；密钥加密密钥均存储在符合GM/T 0028的二级及以上密码模块中。

6.3.3 密钥分发

本单位在密钥分发时均采取身份鉴别、数据完整性、数据机密性等安全措施，均能够抗截取、假冒、篡改、重放等攻击，保证密钥的安全性。

6.3.4 密钥导入与导出

本单位已采取安全措施，防止密钥导入导出时被非法获取或篡改，并保证密钥的正确性。

6.3.5 密钥使用

本单位在密钥使用时已明确用途，并按用途正确使用；对于公钥密码体制，在使用公钥之前均对其进行验证；均有安全措施防止密钥的泄露和替换；密钥泄露时，立即停止使用，并启动相应的应急处理和响应措施。密钥使用时均按照密钥更换周期要求更换密钥；已采取有效的安全措施，保证密钥更换时的安全性。

6.3.6 密钥备份与恢复

本单位已制定明确的密钥备份策略，采用安全可靠的密钥备份恢复机制，对密钥进行备份或恢复；密钥备份或恢复应进行记录，生成审计信息；审计信息包括备份或恢复的主体、备份或恢复的时间等。

6.3.7 密钥归档

本单位已采取有效的安全措施，保证归档密钥的安全性和正确性；归档密钥只能用于解密该密钥加密的历史信息或验证该密钥签名的历史信息；密钥归档应进行记录，并生成审计信息；审计信息包括归档的密钥、归档的时间等；归档密钥应进行数据备份，并采用有效的安全保护措施。

6.3.8 密钥销毁

本单位已具有在紧急情况下销毁密钥的措施。

6.4 建设运行

系统的建设运行过程中，应注意的以下8点：

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。

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。

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。

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。

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。

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。

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。

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。

6.5 密码软硬件及介质管理

认真执行岗位责任制和相关规章制度。

严格遵守安全操作规程，保证密码设备的安全运行。

及时准确地填写各项原始记录和统计报表，并及时反馈密码设备存在的问题。

密码设备操作人员必须经过培训，并留存培训记录。

密码设备操作应由密码操作人员进行，禁止任何非专业人员对机房设备进行任何操作。

密码设备操作应严格遵守相关规章制度和操作规范。

密码设备操作应由两人或两人以上互相监督操作运行，确保操作正确。

密码设备操作前应检查，操作后应查看策略，确保业务能够正常运行。

对于可能影响业务的操作，操作前需要提前进行测试，或在专业人员配合下操作，确保安全后方可执行。

严禁在各密码设备或管理客户端上安装一切与操作无关的软件。

严禁将来历不明的移动存储介质（含光盘、磁盘、优盘等）在密码设备、管理客户端上使用。

操作时若需要连接笔记本电脑操作，应制定操作密码专用笔记本进行操作，专用笔记本应由专人保管，并设置复杂度较高的口令，由操作人员进行管理。设备应严禁安装与操作无关的任何软件等。操作专用笔记本禁止连接外网；专用笔记本电脑应当安装防病毒软件并定期更新，更新时应使用优盘通过补丁进行更新，确保系统安全。

厂家人员操作，应用相关技术人员全程陪同监督。

若需要远程操作，应由相关人员提出申请，经审批后方可执行。厂家人员远程操作，应确保两人及以上同时进行远程操作，同时由相关技术人员陪同并得到证实。

在申请数字证书时应提供真实、完整、准确的身份信息和其他相关信息，并在这些信息变更时及时到与密码小组管理员沟通变更手续；

获取数字证书时，应当使用安全的工具产生并存储私钥及证书，比如使用USB Key来存储数字证书；使用完USB Key后应立即将其从电脑上拔出，不要将USB Key长时间留在电脑上；不使用已被证实产生弱私钥的工具来产生私钥。

设置密码口令时，避免设置与个人资料相关的简单口令，如身份证号码、出生日期、电话号码等，应定期更改口令；

务必妥善保管数字证书使用密码口令及存储数字证书的USB Key设备，防止机密信息泄漏或被他人窃取；如果数字证书遗失，或者发现相关的密码泄漏，务必及时到申请网点办理挂失手续并按照规定重新办理证书和/或设置密码；

避免在公共场所或他人计算机上使用数字证书；

在使用数字证书的电脑上要及时安装操作系统和浏览器的最新安全补丁，提高系统安全性；安装个人防火墙，防止他人的非法访问和恶意攻击；安装并定期更新防病毒软件，防止受到新病毒的侵害；切勿在使用数字证书的电脑上随意登陆不明网络站点，下载、安装不明软件或运行不明程序。

6.6 应急方案

根据《基本要求》中安全管理应急方面的要求，系统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。

6.6.1 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。

（2） 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。

2、 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

（2） 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

（3） 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

6.6.2 应急处置组织机构与职责

1、密码服务组织机构

系统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）。

2、应急响应领导小组

系统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

3、 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

4、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

6.6.3 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；  充分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** | 有心攻击信息系统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。 |

2、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。 |

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。  没有及时申请新的IP或域名证书，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。 |

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机密性、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；  定期查看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.安全与合规性分析

**密码应用合规性对照表**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **指标要求** | **密码技术应用点** | **GB/T 39786密码应用基本要求** | **适用情况（适用/不适用）** | **采取的密码保障措施** | **说明**  **（如采取的缓解及替代性措施）** | **自评结果（通过/不通过）** |
| 物理和环境安全 | 身份鉴别 | 宜 | 适用 |  |  | 通过 |
| 电子门禁记录数据存储完整性 | 宜 | 适用 |  |  | 通过 |
| 视频监控记录数据存储完整性 | 宜 | 适用 |  |  | 通过 |
| 网络和通信安全 | 身份鉴别 | 应 | 适用 |  |  | 通过 |
| 通信数据完整性 | 宜 | 适用 |  |  | 通过 |
| 敏感信息或通信报文的机密性 | 应 | 适用 |  |  | 通过 |
| 网络边界访问控制信息的完整性 | 宜 | 适用 |  |  | 通过 |
| 安全接入认证 | 可 | 不适用 |  |  | 通过 |
| 设备和计算安全 | 身份鉴别 | 应 | 适用 |  |  | 通过 |
| 安全的信息传输通道 | 应 | 适用 |  |  | 通过 |
| 系统资源访问控制信息完整性 | 宜 | 适用 |  |  | 通过 |
| 重要信息资源安全标记完整性 | 宜 | 不适用 |  |  | 通过 |
| 日志记录完整性 | 宜 | 适用 |  |  | 通过 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 宜 | 适用 |  |  | 通过 |
| 应用和数据安全 | 身份鉴别 | 应 | 适用 |  |  | 通过 |
| 访问控制信息完整性 | 宜 | 适用 |  |  | 通过 |
| 重要信息资源安全标记完整性 | 宜 | 不适用 |  |  | 通过 |
| 重要数据传输机密性 | 应 | 适用 |  |  | 通过 |
| 重要数据存储机密性 | 应 | 适用 |  |  | 通过 |
| 重要数据传输完整性 | 宜 | 适用 |  |  | 通过 |
| 重要数据存储完整性 | 宜 | 适用 |  |  | 通过 |
| 不可否认性 | 宜 | 不适用 |  |  | 通过 |
| 管理制度 | 具备密码应用安全管理制度 | 应 | 适用 | 建立密码应用安全管理制度 | 无 | 通过 |
| 密钥管理规则 | 应 | 适用 | 建立密钥管理规则 | 无 | 通过 |
| 建立操作规程 | 应 | 适用 | 建立密码操作规程 | 无 | 通过 |
| 定期修订安全管理制度 | 应 | 适用 | 定期修订安全管理制度 | 无 | 通过 |
| 明确管理制度发布流程 | 应 | 适用 | 明确制度发布流程 | 无 | 通过 |
| 制度执行过程记录留存 | 应 | 适用 | 制度执行过程记录留存 | 无 | 通过 |
| 人员管理 | 了解并遵守密码相关法律法规和密码管理制度 | 应 | 适用 | 要求相关人员了解并遵守密码相关法律法规和密码管理制度 | 无 | 通过 |
| 建立密码应用岗位责任制度 | 应 | 适用 | 建立密码应用岗位责任制度 | 无 | 通过 |
| 建立上岗人员培训制度 | 应 | 适用 | 建立上岗人员培训无制度 | 无 | 通过 |
| 定期进行安全岗位人员考核 | 应 | 适用 | 定期进行安全岗位人员培训 | 无 | 通过 |
| 建立关键岗位人员保密制度和调离制度 | 应 | 适用 | 明确制度发布流程 | 无 | 通过 |
| 建设运行 | 制定密码应用方案 | 应 | 适用 | 制定密码应用方案 | 无 | 通过 |
| 制定密钥安全管理策略 | 应 | 适用 | 制定密钥安全管理策略 | 无 | 通过 |
| 制定实施方案 | 应 | 适用 | 制定实施方案 | 无 | 通过 |
| 投入运行前进行密码应用安全性评估 | 应 | 适用 | 投入运行前密码应用安全性评估 | 无 | 通过 |
| 定期开展密码应用安全性评估及攻防对抗演习 | 应 | 适用 | 定期开展密码应用安全性评估及攻防对抗演习 | 无 | 通过 |
| 应急处置 | 应急策略 | 应 | 适用 | 制定应急策略 | 无 | 通过 |
| 事件处置 | 应 | 适用 | 制度事件处置流程 | 无 | 通过 |
| 向有关主管部门上报处置情况 | 应 | 适用 | 向有关主管部门上报处置情况 | 无 | 通过 |

8.实施保障方案

8.1 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。

8.1.1 软硬件开发及改造

按照采购内容和本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。

8.1.2 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。

8.1.3 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。

8.1.4 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。

8.1.5 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。

8.1.6 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。

(2)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。

2、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。

(2)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。

8.2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。

8.2.1 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。

8.2.2 进度计划

本项目主要阶段实施工作分解如表7.1所示：

表 7.1 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 |

8.3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、监督检查五个方面。

8.3.1 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。

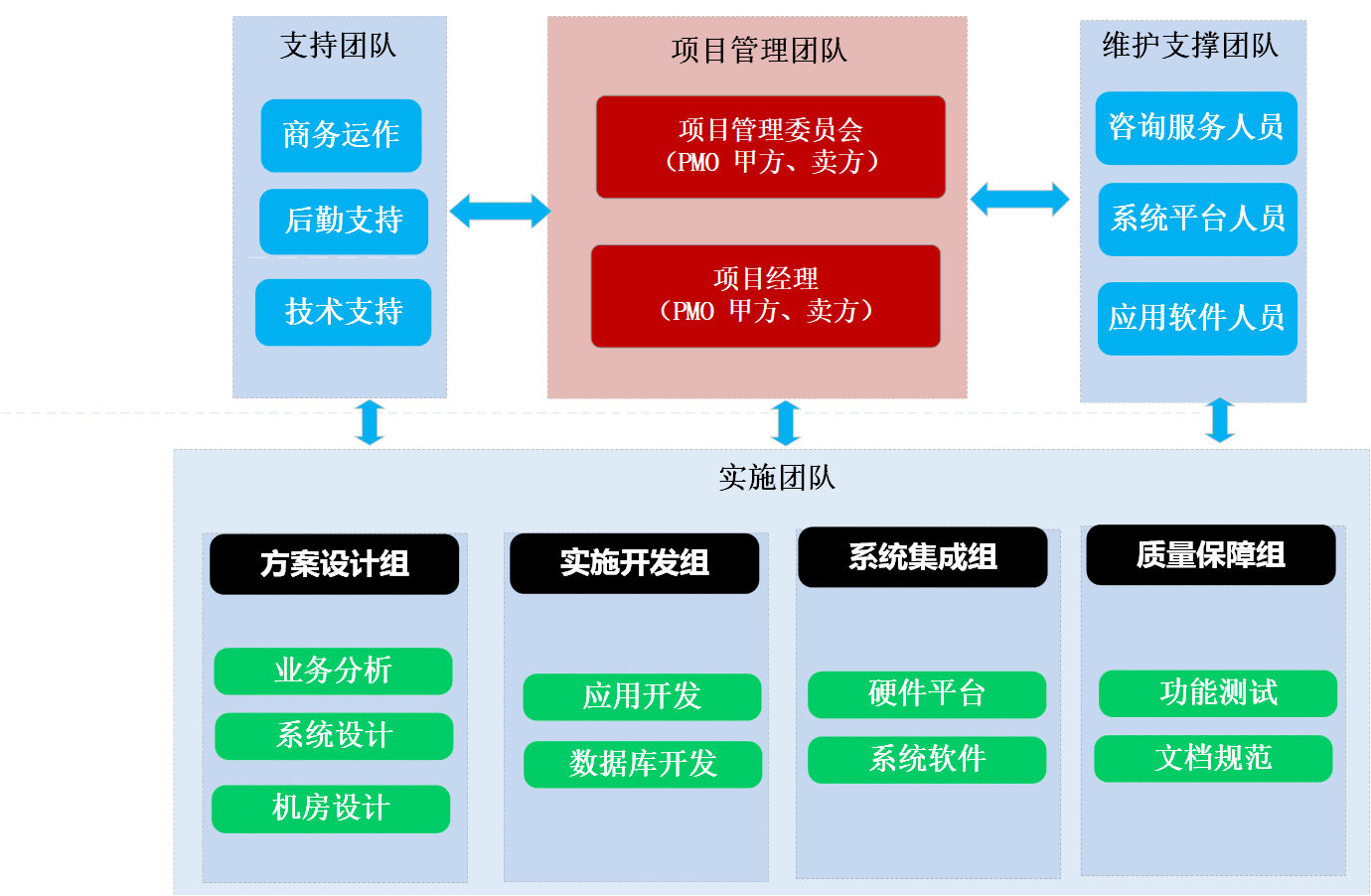


图 7.1 组织架构图

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，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，收集、分析、汇总用户需求，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，与实施开发组配合工作。配合买方负责对整体机房做整体建设设计，输出建设图纸。
  2. 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，包括应用的开发和数据库的开发。
  3. 系统集成组：负责设备平台的架设、安装、调试，同时配合实施开发组将开发完成的软件及第三方软件有效的集成发布在测试、生产环境，并确保调试通过。
  4. 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。完成系统集成后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；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. 咨询服务人员：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. 系统平台人员：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. 应用软件人员：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。支持团队职责包括：

* 1. 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。；负责整个项目的后勤支持，减少项目组的无效投入；
  2. 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。

8.3.2 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。

8.3.3 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。

8.3.4 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（以下简称“SQA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。

8.3.5 监督检查

**监督检查的重点：**

(一) 工作任务是否得到全面落实，包括任务分解、项目前期准备、项目开工、项目客观真实性等情况。

(二)基本建设程序和强制性标准是否得到严格执行，包括建设程序是否合规，实施质量是否符合规定和强制性标准，实施建设进度、资料文档是否符合要求等。

**监督检查的原则：**

(一)统一组织，分工负责。

(二)统筹兼顾，突出重点。既要保证监督检查能够覆盖项目实施的主要方面，又要紧盯突出问题、抓住关键环节，选准着力点，切实增强监督检查的针对性和有效性。

(三)通盘谋划、分类实施。要从项目全局出发考虑和处理问题，实事求是地确定检查内容，切实增强监督检查的科学性和合理性。

(四)查纠结合，务求实效。

**监督检查的措施：**

(一)建立常态化监督检查机制，进入被检查单位和施工现场进行检查。

(二)询问被检查单位工作人员，要求其说明有关情况。

(三)要求被检查单位提供有关工程质量的文件和材料。

(四)对电子元器件、硬件设备、工程实体质量进行抽样检测。

(五)对发现的质量问题，责令改正，视情节对责任单位采取通报批评等处理措施。

8.4经费概算

根据XXX系统物理和环境、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、制定的密码方案的内容以及产品清单内容，密码应用建设的密码产品及配套服务预算表如表8.4所示。

表 8.4 密码产品及配套服务预算表

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 产品/服务 | 数量  (台/套) | 单价  (万元) | 预算  (万元) | 备注 |
| 1 | 服务器密码机 |  |  |  |  |
| 2 | 签名验签服务器 |  |  |  |  |
| 3 | 国密安全密码应用中间件 |  |  |  |  |
| 4 | 国密数字证书 |  |  |  |  |
| 5 | 智能密码钥匙 |  |  |  |  |
| 6 | SSL VPN安全网关 |  |  |  |  |
| 7 | 密钥管理系统 |  |  |  |  |
| 8 | 密码应用技术服务 | 1 |  |  |  |
| **总计** | | | |  |  |