**XX人工智能超算中心HPC超级计算集群系统**

**密码应用方案**

项 目 名 称：XX人工智能超算中心（一期）设备采购及建设（含设计）项目

项目建设单位

编制单位：

编 制 日 期： 二〇二三年三月

目录

[**1 背景** 1](#_Toc131608477)

[**2 系统概述** 2](#_Toc131608478)

[**2.1 基本情况** 2](#_Toc131608479)

[**2.2 系统网络拓扑** 3](#_Toc131608480)

[**2.3 承载的业务情况** 4](#_Toc131608481)

[**2.4 系统软硬件构成** 7](#_Toc131608482)

[**2.4.1 物理环境** 7](#_Toc131608483)

[**2.4.2 物理安防设施** 7](#_Toc131608484)

[**2.4.3 密码产品** 8](#_Toc131608485)

[**2.4.4 服务器/存储设备** 8](#_Toc131608486)

[**2.4.5 网络及安全设备** 9](#_Toc131608487)

[**2.4.6 关键业务系统** 10](#_Toc131608488)

[**2.4.7 重要数据** 10](#_Toc131608489)

[**2.5管理制度** 10](#_Toc131608490)

[**3 密码应用需求分析** 11](#_Toc131608491)

[**3.1 物理和环境安全** 11](#_Toc131608492)

[**3.2 网络和通信安全** 12](#_Toc131608493)

[**3.3 设备和计算安全** 13](#_Toc131608494)

[**3.4 应用和数据安全** 14](#_Toc131608495)

[**3.5 密钥管理** 15](#_Toc131608496)

[**3.6 安全管理** 15](#_Toc131608497)

[**3.7 需求分析** 16](#_Toc131608498)

[**4 设计目标及原则** 19](#_Toc131608499)

[**4.1 设计目标** 19](#_Toc131608500)

[**4.2 设计原则与依据** 19](#_Toc131608501)

[**4.2.1 设计原则** 19](#_Toc131608502)

[**4.2.2 主要依据** 20](#_Toc131608503)

[**5 总体设计方案** 22](#_Toc131608504)

[**6 详细方案设计** 23](#_Toc131608505)

[**6.1 物理和环境安全** 23](#_Toc131608506)

[6.1.1 总体要求 23](#_Toc131608507)

[6.1.2 功能设计 24](#_Toc131608508)

[**6.2 网络和通信安全** 27](#_Toc131608509)

[6.2.1 总体要求 27](#_Toc131608510)

[6.2.2 功能设计 27](#_Toc131608511)

[**6.3 设备和计算安全** 28](#_Toc131608512)

[6.3.1 总体要求 28](#_Toc131608513)

[6.3.2 功能设计 28](#_Toc131608514)

[**6.4 应用和数据安全** 30](#_Toc131608515)

[6.4.1 总体要求 30](#_Toc131608516)

[6.4.2 功能设计 30](#_Toc131608517)

[**6.5 密钥管理安全** 32](#_Toc131608518)

[**6.5.1 国密身份认证系统** 32](#_Toc131608519)

[**6.5.2 SSL VPN安全网关密钥管理** 34](#_Toc131608520)

[**6.5.3 传输透明加密系统** 38](#_Toc131608521)

[**6.5.4 服务器密码机密码密钥管理** 40](#_Toc131608522)

[**6.6 密码应用流程** 43](#_Toc131608523)

[**6.6.1 国密身份认证流程** 43](#_Toc131608524)

[**6.6.2 SSL VPN安全网关管理流程** 43](#_Toc131608525)

[**6.6.3 传输透明加密系统流程说明** 44](#_Toc131608526)

[**6.6.4 服务器密码机流程说明** 45](#_Toc131608527)

[**6.7 安全与合规性分析** 49](#_Toc131608528)

[**6.8 密码应用部署** 55](#_Toc131608529)

[**6.9 密码软硬件产品清单** 56](#_Toc131608530)

[**7 安全管理方案** 57](#_Toc131608531)

[**7.1 密码应用安全管理制度** 57](#_Toc131608532)

[**7.1.1 总则** 57](#_Toc131608533)

[**7.1.2 制定和发布** 57](#_Toc131608534)

[**7.1.3 评审和修订** 58](#_Toc131608535)

[**7.1.4 附则** 59](#_Toc131608536)

[**7.1.5 附件** 59](#_Toc131608537)

[**7.2 密码应用安全操作规程** 62](#_Toc131608538)

[**7.2.1 总则** 62](#_Toc131608539)

[**7.2.2 密码应用相关人员操作规程** 62](#_Toc131608540)

[**7.2.3 附则** 63](#_Toc131608541)

[**7.3 密码软硬件及介质管理制度** 64](#_Toc131608542)

[**7.3.1 总则** 64](#_Toc131608543)

[**7.3.2 密码产品安全及管理** 64](#_Toc131608544)

[**7.3.3 终端设备安全管理** 66](#_Toc131608545)

[**7.3.4 设备的物理安全** 67](#_Toc131608546)

[**7.3.5 介质管理** 67](#_Toc131608547)

[**7.4 密码应用安全组织机构管理制度** 69](#_Toc131608548)

[**7.4.1 总则** 69](#_Toc131608549)

[**7.4.2 组织架构** 69](#_Toc131608550)

[**7.4.3 岗位职责** 70](#_Toc131608551)

[**7.5 密码应用安全人员管理制度** 76](#_Toc131608552)

[**7.5.1 总则** 76](#_Toc131608553)

[**7.5.2 岗位配置原则** 76](#_Toc131608554)

[**7.5.3 人员录用及调离** 77](#_Toc131608555)

[**7.5.4 培训与考核** 78](#_Toc131608556)

[**7.5.5 附件** 79](#_Toc131608557)

[**7.6 密码应用建设运行管理制度** 87](#_Toc131608558)

[**7.6.1 规划建设** 87](#_Toc131608559)

[**7.6.2 运行维护** 87](#_Toc131608560)

[**7.6.3 备份与恢复** 88](#_Toc131608561)

[**7.7 密码应用安全应急管理制度** 89](#_Toc131608562)

[**7.7.1 总则** 89](#_Toc131608563)

[**7.7.2 事件分类定级** 89](#_Toc131608564)

[**7.7.3 事件处理程序** 90](#_Toc131608565)

[**7.8 密钥安全管理规范** 92](#_Toc131608566)

[**7.8.1 密钥设备管理规范** 92](#_Toc131608567)

[**7.8.2 密钥生命周期的安全管理** 92](#_Toc131608568)

[**7.8.3 管理规定与监督检查** 94](#_Toc131608569)

[**7.8.4 附则** 96](#_Toc131608570)

[**8 实施保障方案** 96](#_Toc131608571)

[**8.1 项目组织架构** 96](#_Toc131608572)

[**8.2 组织职责说明** 97](#_Toc131608573)

[**8.2.1 项目经理** 97](#_Toc131608574)

[**8.2.2 项目协调管理小组（质量负责人、项目技术负责人）** 97](#_Toc131608575)

[**8.2.3 安全服务组（技术人员）** 98](#_Toc131608576)

[**8.2.4 产品实施小组（售后工程师）** 98](#_Toc131608577)

[**8.2.5 文档小组** 98](#_Toc131608578)

[**8.3 检查监督管理** 99](#_Toc131608579)

[**8.4 项目质量保障** 99](#_Toc131608580)

**1 背景**

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。《中华人民共和国密码法》的颁布实施，从法律层面为开展商用密码应用提供了根本遵循，《国家政务信息化项目建设管理办法》的颁布实施，进一步促进了商用密码的全面应用。

为贯彻落实《中华人民共和国密码法》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》，XX人工智能超算中心HPC超级计算集群系统需进行密码应用建设。根据我国颁布的《密码法》、《商用密码管理条例》等相关法律条例，各类信息系统中涉及密码应用的部分应符合国家密码管理局相关标准，XX人工智能超算中心HPC超级计算集群系统应满足商用密码应用安全性测评的要求。

通过对XX人工智能超算中心HPC超级计算集群系统的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》，本应用方案将分别从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等4个层面，以及密钥管理、安全管理等方面，设计此次XX人工智能超算中心HPC超级计算集群系统密码应用的技术方案、安全管理方案和实施保障方案。建设符合《中华人民共和国密码法》以及GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的信息系统，实现对保护对象（重要业务数据、鉴别数据、重要日志数据等）的机密性、完整性、真实性保护。

**2 系统概述**

**2.1 基本情况**

XX人工智能超算中心HPC超级计算集群系统采用模块化分布式架构，提供HPC超算全方位的作业调度、集群监控管理等功能，整合国内外应用软件，建设超算应用商城，通过API为高校、科研院所、企事业单位和ISV等用户提供后台算力支撑。

系统建设单位为XX宁数智能计算产业发展有限公司，单位地址为XXX，所属密码管理部门为XX市密码管理局，系统建设单位类型为国企。

XX人工智能超算中心HPC超级计算集群系统于2023年2月09日完成网络安全等级保护定级备案，定级等级为第三级。

**2.2 系统网络拓扑**

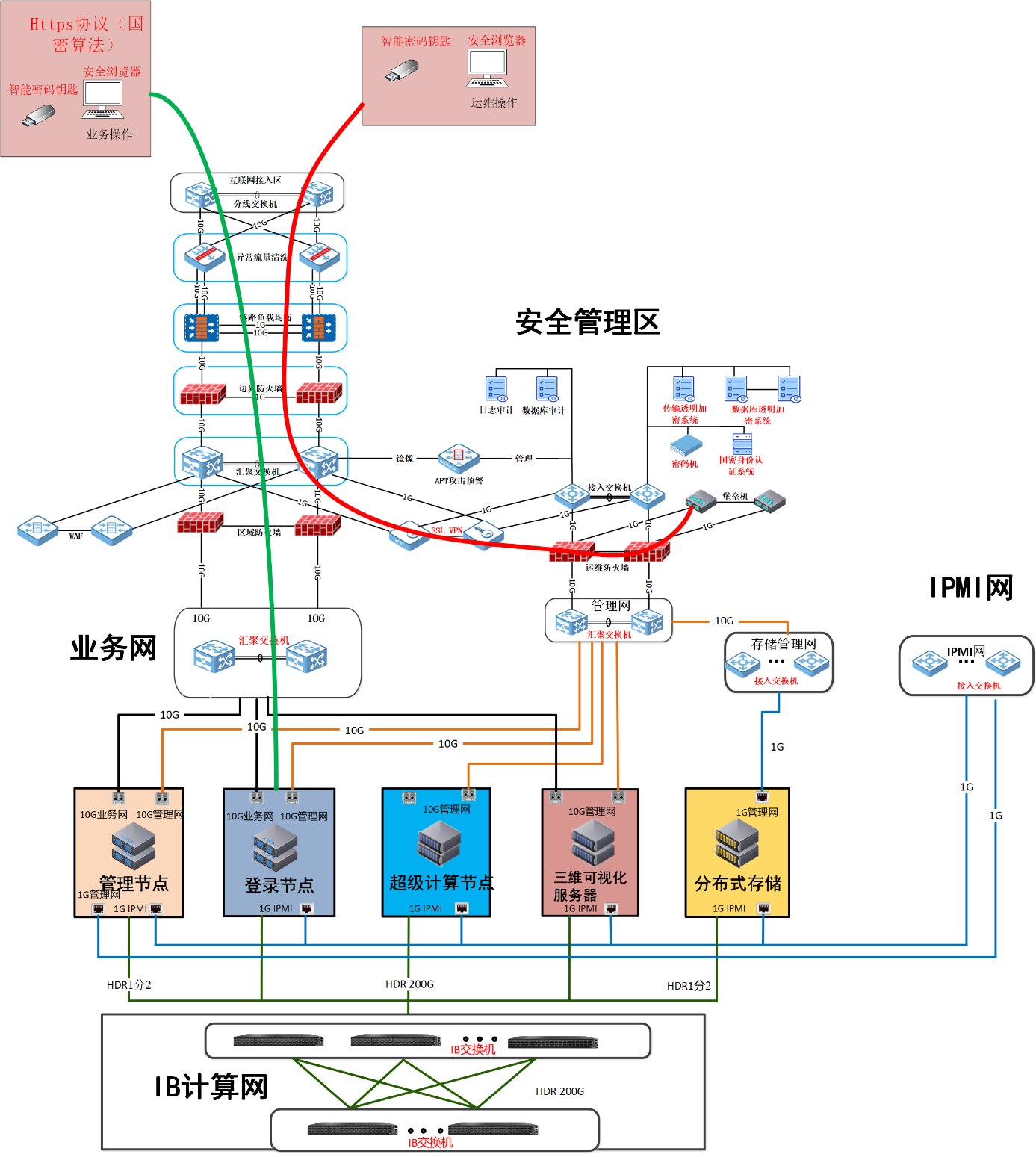


图2-1 XX人工智能超算中心HPC超级计算集群系统网络拓扑图

本系统分为互联网接入区、运维管理区、服务器区三大部分，其中互联网接入区主要包含防火墙、WAF、DDOS设备、APT攻击预警等安全防护设备以及SSL VPN等安全接入设备，运维管理区主要包含数据库审计、日志审计、堡垒机等审计类设备以及密码机、身份认证等密码设备，服务器区主要部署AC登录系统以及计算和存储节点，为用户提供计算服务。

业务用户通过浏览器访问AC平台，进行业务作业提交,用户配备USB Key，通过国密身份认证系统实现双因素认证登录，保障登录用户身份的真实性；部署传输透明加密系统，用户终端动态加载加解密算法模块，实现数据在浏览器页面加密；通过部署云密盾密码管理系统，采用SM4-CBC算法实现用户注册信息（个人姓名、手机号码、单位信息、账号口令）进行机密性保护，并使用HMAC-SM3算法对用户注册信息（个人姓名、手机号码、单位信息、账号口令）、日志数据等重要数据进行完整性保护。

运维人员通过SSL VPN 接入系统内部访问堡垒机，通过堡垒机进行运维管理操作, SSL VPN安全网关采用基于国产密码算法（SM2、SM3、SM4）的SSL协议进行通信，通过SM2算法实现对通信双方进行身份鉴别，利用HMMA-SM3算法保障通信数据完整性，利用SM4算法保障通信过程中重要数据的机密性。

**2.3 承载的业务情况**

XX人工智能超算中心HPC超级计算集群系统主要包含计算、存储、网络等硬件基础设施，软件平台及应用服务能力，安全系统等建设内容以及机房、电气、弱电等基础配套设施。系统对不同的保护对象从物理环境防护、通信网络防护、区域边界防护、计算环境防护等各方面进行安全防护，达到三级防护要求，为不同用户提供安全可靠的算力支撑服务，本系统不涉及敏感业务数据存储。

XX人工智能超算计算集群的IT基础设施拟采用异构体系架构，其核心单元包含以国产通用CPU处理器、高性能计算节点组成的超算子系统，提供5PFLOPs超算算力。超级计算集群同时配套满足国家网络安全等级保护的安全组件。

超算中心系统全面考虑科学计算等不同业务的需求特点，以及科学计算、大数据等多种计算架构交叉耦合的现状和未来的发展趋势，科学有效设计和配置系统硬件结构，从而使硬件配置架构和应用软件的需求特性相匹配，最大限度地发挥硬件的能力，提高运算效率，并满足未来发展和系统升级的要求。超算中心子系统按功能模块分为科学计算单元、液冷配套单元等部分。

超算计算单元包含120个国产科学计算节点，每个科学计算节点包含1个CPU处理器和4个异构加速卡，提供43TFLOPs（FP64）多的科学计算算力，120个共组成5 PFLOPs（FP64）多的算力集群。

依托XX人工智能超算中心的算力，满足XX市产业、科研、社会治理等各领域的算力需求，并加速数字化和智能化产业集聚，构建XX数字产业生态，积极赋能和驱动XX数字经济、智能产业、智慧城市、智慧社会发展。在城市治理、公共服务及公共安全等方面提供解决方案，消除隐患、提供新的服务或提升业务效率。具体在政府各个职能机构中有许多应用场景，例如：

城市管理局：自动识别占道经营、乱堆物料等、自动预警

公安局：智能监控、侦查辅助

自规局：空间规划、生态修复、执法督查

农业局：农情监测、农作物估产、农业保险

住建局：城市环境监测、城市沉降监测

气象局：气象预测

环保局：生态环境监测与评价

业务流程描述：

业务用户通过浏览器访问AC平台，进行业务作业提交,用户配备USB Key，通过国密身份认证系统实现双因素认证登录，保障登录用户身份的真实性；部署传输透明加密系统，用户终端动态加载加解密算法模块，实现数据在浏览器页面加密；通过部署服务器密码机，采用SM4-CBC算法实现用户注册信息（个人姓名、手机号码、单位信息、账号口令）进行机密性保护，并使用HMAC-SM3算法对用户注册信息（个人姓名、手机号码、单位信息、账号口令）、日志数据等重要数据进行完整性保护。

运维人员通过SSL VPN 接入系统内部访问堡垒机，通过堡垒机进行运维管理操作, SSL VPN安全网关采用基于国产密码算法（SM2、SM3、SM4）的SSL协议进行通信，通过SM2算法实现对通信双方进行身份鉴别，利用HMMA-SM3算法保障通信数据完整性，利用SM4算法保障通信过程中重要数据的机密性。

**2.4 系统软硬件构成**

XX超算集群系统有计算机终端、服务器、交换机、防火墙等硬件资源和操作系统、数据库、中间件等软件资源。

**2.4.1 物理环境**

表2-1物理环境

| 序号 | 物理环境名称 | 物理位置 | 重要程度 |
| --- | --- | --- | --- |
| 1 | 本地机房 | XXX | 最高 |

**2.4.2 物理安防设施**

表2-2物理安防设施

| 序号 | 产品名称 | 生产厂商和型号 | 商密产品认证证书编号 | 所在物理环境名称 | 重要程度 |
| --- | --- | --- | --- | --- | --- |
| 1 | 安全管理一体机 | 海康威视/SHT1810 | GM003319920200856 | 本地机房 | 重要 |
| 2 | 硬盘录像机NVR | 海康威视/SJT1809 | GM003319920201016 | 本地机房 | 重要 |
| 3 | PSAM卡 | 复旦微电子/SSX1813 | GM003119920200963 | 本地机房 | 重要 |
| 4 | CPU卡 | 复旦微电子/SJK1214 | GM003119920201508 | 本地机房 | 重要 |

**2.4.3 密码产品**

表2-3 密码产品

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 产品名称 | 生产厂商 | 商密产品认证证书编号 | 使用的密码算法 | 数量 | 用途 |
| 1 | SSL VPN | 中宇万通 | GM001110620202094 | SM2/SM3/SM4 | 2 | 远程接入 |
| 2 | 国密身份认证系统 | 弗兰科 | GM003319920201080 | SM2/SM3/SM4 | 1 | 身份鉴别 |
| 3 | 密码机 | 弗兰科 | GM003311020210408 | SM2/SM3/SM4 | 2 | 提供密钥产生、加密以及解密服务 |
| 4 | 传输透明加密系统 | 弗兰科 | GM003312220220253 | SM2/SM3/SM4 | 1 | 应用层数据传输加密 |

**2.4.4 服务器/存储设备**

表2-4 服务器/存储设备

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 生产厂商 | 型号 | 操作系统版本 | 是否为虚拟设备 | 用途 | 数量 | 重要程度 |
| **1** | 浸没液冷超算刀箱 | 中科可控 | TC8600H | 中科方德/NFS3.2 | 否 | 计算节点刀箱 | 6 | 重要 |
| **2** | 浸没液冷超算刀片 | 中科可控 | TC8600H | 中科方德/NFS3.2 | 否 | 高性能计算节点 | 60 | 重要 |
| **3** | 分布式存储 | 中科可控 | TC8600H | CentOS  7.5 | 否 | 数据存储 | 20 | 重要 |
| **4** | 服务器I/登入管理节点 | 中科可控 | TC8600H | 中科方德/NFS3.2 | 否 | 管理节点 | 13 | 重要 |
| **5** | 服务器II/GPU节点 | 中科可控 | TC8600H | 中科方德/NFS3.2 | 否 | 登录节点 | 2 | 重要 |

**2.4.5 网络及安全设备**

表2-5 网络及安全设备

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| 序号 | 设备名称 | 生产厂商 | 型号 | 用途  （包括涉及的密码技术） | 数量 | 重要程度 |
|  | 异常流量清洗网关设备 | 中科曙光 | HAFFirm-Z20K | 异常流量清洗系统 | 2 | 重要 |
|  | 边界防火墙 | 中科曙光 | TLFW-2000-S60 | 边界网络系统 | 2 | 重要 |
|  | 区域防火墙 | 中科曙光 | TLFW-2000-S60 | 区域网络系统 | 2 | 重要 |
|  | 运维防火墙 | 中科曙光 | TLFW-2000-S41 | 运维网络系统 | 2 | 重要 |
|  | 负载均衡 | 中科曙光 | DCLB-8600AD | 负载均衡系统 | 2 | 重要 |
|  | SSL VPN | 中宇万通 | SG-5200 | 用户接入系统 | 2 | 重要 |
|  | 堡垒机 | 中科曙光 | OperaFirm-X1040 | 用户管理系统 | 2 | 重要 |
|  | 日志审计 | 天融信 | TA-L-HSE-G100 | 日志审计系统 | 1 | 重要 |
|  | 数据库审计 | 天融信 | TA-55629-DB | 数据库审计系统 | 1 | 重要 |
|  | Web应用防护系统 | 天融信 | TWF-72280 | Web应用系统 | 2 | 重要 |
|  | APT攻击预警平台 | 安恒 | DAS-APT-5000 | APT防护系统 | 1 | 重要 |
|  | 计算存储网络交换机 | 迈络思 | MS8790 | 计算和存储网络 | 6 | 重要 |
|  | 核心交换机 | 锐捷 | RG-N18010-X | 网络核心层 | 2 | 重要 |
|  | 汇聚交换机 | 锐捷 | RG-S6250-48XS8CQ | 网络汇聚层 | 10 | 重要 |
|  | 接入交换机 | 锐捷 | RG-2910-48GT4XS-E | 网络接入层 | 10 | 重要 |

**2.4.6 关键业务系统**

表2-6 关键业务系统清单

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 应用名称 | 版本 | 部署位置 | 主要功能 |
| 1 | HPC集群管理软件 | V6.0 | 刀片服务器、登入管理节点、GPU节点 | 集群管理 |
| 2 | 超算调度平台 | V6.0 | 刀片服务器、登入管理节点、GPU节点 | 应用调度 |
| 3 | 超算运营平台 | V6.0 | 刀片服务器、登入管理节点、GPU节点 | 平台运营 |

**2.4.7 重要数据**

表2-7 系统重要数据清单

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 序号 | 数据 | 描述 | 所属应用 | 存储位置 | 安全需求 |
| 1 | 用户注册信息 | 个人的姓名、手机号码、单位、账号、密码 | XX超算集群系统 | AC数据库 | 机密性、完整性 |
| 2 | 日志数据 | 运维操作日志 | XX超算集群系统 | 堡垒机 | 完整性 |
| 3 | 日志数据 | VPN登录日志 | XX超算集群系统 | VPN | 完整性 |

**2.5管理制度**

XX宁数智能计算产业发展有限公司根据《信息安全技术 信息系统密码应用基本要求》（GB/T39786-2021）的三级要求，从管理制度、人员管理、建设运行和应急处置四个层面制定了相应的制度文件、规章流程，保障系统规划、建设、后期运维和应急响应的安全性。主要管理制度如下：

《XX人工智能超算中心HPC超级计算集群系统密码应用安全管理制度》

《XX人工智能超算中心HPC超级计算集群系统密码软硬件及介质管理制度》

《XX人工智能超算中心HPC超级计算集群系统密码应用组织机构管理制度》

《XX人工智能超算中心HPC超级计算集群系统密码应用安全人员管理制度》

《XX人工智能超算中心HPC超级计算集群系统密码应用建设运行管理制度》

《XX人工智能超算中心HPC超级计算集群系统密码应用安全应急管理制度》

**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》，从物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、安全管理等层面，对XX超算集群系统进行综合的风险分析，得出所存在的密码应用需求。

**3.1 物理和环境安全**

1．风险分析

（1）身份鉴别：机房门禁系统通过门禁卡对进出人员进行身份鉴别，未使用密码技术的真实性功能来保护物理访问控制身份鉴别信息。

（2）电子门禁记录数据完整性：机房对门禁进出记录数据进行管理，未使用密码技术对人员进出记录进行完整性保护。

（3）视频记录数据完整性：机房未使用密码技术对视频监控音像记录进行完整性保护。

2．密码应用需求

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，XX人工智能超算中心HPC超级计算集群系统的物理和环境安全需求如下：

（1）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。

（2）采用密码技术保证电子门禁系统进出记录数据的存储完整性。

1. 采用密码技术保证视频监控音像记录数据的存储完整性。

**3.2 网络和通信安全**

1. 风险分析

目前本系统用户通过普通浏览器、客户端访问业务系统，数据传输安全隐患，存在接入实体身份不可控，存在通信数据在信息系统外部被非授权截取等风险。

1. 密码应用需求

网络和通信安全主要实现对业务系统与经由外部网络连接的实体、内部跨物理机房通信时进行网络通信安全防护，涉及的密码应用需求主要有:

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，XX人工智能超算中心HPC超级计算集群系统的网络和通信安全需求如下：

（1）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）采用密码技术保证通信过程中数据的完整性。

（3）采用密码技术保证通信过程中重要数据的机密性。

（4）采用密码技术保证网络边界访问控制信息的完整性。

**3.3 设备和计算安全**

1. 风险分析

系统管理员在内网通过堡垒机，使用用户名+口令登录堡垒机，对系统中的应用服务器、数据库服务器、网络设备、安全设备进行运维管理，未使用密码技术对管理员进行身份鉴别，存在非授权人员登录，对系统进行恶意破坏的风险。

1. 密码应用需求

设备和计算安全主要实现对业务系统中物理机、网络设备及安全设备等安全防护，为业务系统所涉及的各类设备提供密码支撑和保障作用，涉及的密码应用需求主要有：

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，XX人工智能超算中心HPC超级计算集群系统的设备和计算安全需求如下：

（1）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。

（2）远程管理设备时，采用密码技术建立安全的信息传输通道。

（3）采用密码技术保证系统资源访问控制信息的完整性。

（4）采用密码技术保证设备中的重要信息资源安全标记的完整性。

（5）采用密码技术保证日志记录的完整性。

（6）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。

**3.4 应用和数据安全**

1. 风险分析

业务系统存在口令泄露被仿冒登录等风险，关键鉴别数据业务数据存在传输、存储过程中被泄露的风险，也潜在存在被非法篡改风险，需保证关键数据机密性、完整性。

1. 密码应用需求

应用和数据安全是业务系统安全防护的核心，涉及的密码应用需求主要有：

依据《GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求》中的第三级信息系统商用密码应用要求，XX人工智能超算中心HPC超级计算集群系统的应用和数据安全安全需求如下：

（1）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。

（2）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）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。

（4）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。

（5）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完整性。

（6）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。

**3.5 密钥管理**

1. 风险分析

系统中的密钥管理面临保护不足带来的密钥泄露风险，密钥泄露潜在会导致被保护数据泄露；针对证书等存在证书到期未及时更新带来的业务中断、安全隐患；针对密钥保护的高安全性，没有通过认证的硬件密码模块，会降低密钥管理安全等级。

2. 密码应用需求

业务系统内使用到的对称密钥、非对称密钥（证书等）需要进行生命周期管理，覆盖密钥的产生、分发、存储、使用、更新、归档、撤销、备份、恢复和销毁等环节，保证密钥（除公钥外）不被非授权的访问、使用、泄露、修改和替换，同时保证公钥不被非授权的修改和替换。

**3.6 安全管理**

1．风险分析

信息安全风险的应对之道，要从制度管理和技术防范两个方面来考虑，二者相辅相成，制度管理在实际安全防护中的地位相对较高，是信息系统安全管理的基础，建立健全各项信息安全制度是进行安全管理的第一步，正如信息安全广泛流传的“三分技术、七分管理”的说法，集中反映的也是这个道理。保障信息系统安全，无论技术防范如何健全，还是要依托管理制度的完善，并最终落实到人的执行效果。

本系统已依据网络安全等级保护第三级系统相关要求制定信息安全管理制度体系，但目前阶段管理制度体系尚未包含密码安全管理相关内容，不利于在本系统中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。

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》第三级别要求，制定本系统密码应用解决方案，并委托密评机构对密码应用解决方案进行评估，评估通过后，建设密码保障系统，制定密码相关的管理制度，系统改造完成后，依据密码应用解决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。

**3.7 需求分析**

表3-1 系统密码应用需求分析清单

| 安全  层面 | 指标要求 | 系统密码应用需求 | 不适用说明 |
| --- | --- | --- | --- |
| 物理和环境安全 | 身份鉴别 | 确认进入机房人员的身份真实性，防止假冒人员进入 | 无 |
| 电子门禁记录数据存储完整性 | 保护电子门禁系统进出记录完整性，防止被非授权篡改 |
| 视频监控记录数据存储完整性 | 保护视频监控音像记录的完整性，防止被非授权篡改 |
| 网络和通信安全 | 身份鉴别 | 确认通信实体的身份真实性，防止与假冒实体进行通信 | 无 |
| 通信数据完整性 | 保护通信过程中重要数据的完整性和机密性，防止数据被非授权篡改，防止敏感数据泄露 | 无 |
| 通信过程中重要数据的机密性 |
| 网络边界访问控制信息的完整性 | 保护网络边界设备中的访问控制信息的完整性，防止被非授权篡改 | 无 |
| 安全接入认证 | 采用密码技术建立安全传输通道，实现客户端与服务端通信实体的身份鉴别 | 无 |
| 设备和计算安全 | 身份鉴别 | 对系统管理员的身份真实性进行识别和确认，防止假冒人员登录 | 无 |
| 远程管理通道安全 | 建立系统安全的数据传输通道 | 无 |
| 系统资源访问控制信息完整性 | 保护计算机、服务器等设备中的系统资源访问控制信息的完整性，防止被非授权篡改 | 无 |
| 重要信息资源安全标记完整性 | 对重要信息资源进行安全标记完整性保护，防止重要资源数据被恶意篡改 | 无 |
| 日志记录完整性 | 保护各类物理设备中的日志记录的完整性，防止被非授权篡改 | 无 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 保护各类物理设备中的重要可执行程序的完整性，并对重要可执行程序来源进行鉴别，防止被非授权篡改 | 无 |
| 应用和数据安全 | 身份鉴别 | 确认PC端登录用户的身份真实性，防止假冒人员登录 | 无 |
| 访问控制信息完整性 | 对访问权限控制列表进行完整性保护，防止被非授权篡改 | 无 |
| 重要信息资源安全标记完整性 | 对重要信息资源进行安全标记完整性保护，防止重要资源数据被恶意篡改 | 无 |
| 重要数据传输机密性 | 保护在应用系统之间的非安全网络信道中传输的和存储的用户登录身份鉴别信息、重要业务数据的机密性和完整性，防止数据泄露给非授权的个人、进程等 | 无 |
| 重要数据存储机密性 |
| 重要数据传输完整性 |
| 重要数据存储完整性 |
| 不可否认性 | 不适用 | 本系统不涉及电子商务、CA认证、网上银行、证券交易、电子合同、电子公文等（可能涉及法律责任认定的应用），目前没有不可否认性保护需求，故无需部署相关密码产品。 |
| 管理制度 | 具备密码应用安全管理制度 | 应具备密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度 | 无 |
| 密钥管理规则 | 应根据密码应用方案建立相应密钥管理规则 | 无 |
| 建立操作规程 | 应对管理人员或操作人员执行的日常管理操作建立操作规程 | 无 |
| 定期修订安全管理制度 | 应定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定,对存在不足或需要改进之处进行修订 | 无 |
| 明确管理制度发布流程 | 应明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制 | 无 |
| 制度执行过程记录留存 | 应具有密码应用操作规程的相关执行记录并妥善保存 | 无 |
| 人员管理 | 了解并遵守密码相关法律法规和密码管理制度 | 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度 | 无 |
| 建立密码应用岗位责任制度 | 应建立密码应用岗位责任制度,明确各岗位在安全系统中的职责和权限  1)根据密码应用的实际情况,设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位  2)对关键岗位建立多人共管机制  3)密钥管理、密码安全审计、密码操作人员职责互相制约互相监督,其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任  4)相关设备与系统的管理和使用账号不得多人共用 | 无 |
| 建立上岗人员培训制度 | 应建立上岗人员培训制度,对于涉及密码的操作和管理的人员进行专门培训,确保其具备岗位所需专业技能 | 无 |
| 定期进行安全岗位人员考核 | 应定期对密码应用安全岗位人员进行考核 | 无 |
| 建立关键岗位人员保密制度和调离制度 | 应建立关键人员保密制度和调离制度,签订保密合同,承担保密义务 | 无 |
| 建设运行 | 制定密码应用方案 | 应依据密码相关标准和密码应用需求,制定密码应用方案 | 无 |
| 制定密钥安全管理策略 | 应根据密码应用方案,确定系统涉及的密钥种类、体系及其生存周期环节 | 无 |
| 制定实施方案 | 应按照应用方案实施建设 | 无 |
| 投入运行前进行密码应用安全性评估 | 投入运行前进行密码应用安全性评估，评估通过后系统方可正式运行 | 无 |
| 定期开展密码应用安全性评估 | 在运行过程中，应严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及功放对抗演习，并根据评估结果进行整改 | 无 |
| 应急处置 | 应急策略 | 应制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置 | 无 |
| 事件处置 | 事件发生后，应及时向信息系统主管部门进行报告 | 无 |
| 向有关主管部门上报处置情况 | 事件处置完成后，应及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况 | 无 |

**4 设计目标及原则**

**4.1 设计目标**

根据GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》中第三级密码应用基本要求，综合考虑XX人工智能超算中心HPC超级计算集群系统在物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全、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，满足密码应用安全性评估的要求。

**4.2 设计原则与依据**

**4.2.1 设计原则**

密码应用设计应遵循以下原则：

（1）**总体性原则。**通过从整体层面，对本平台的密码应用开展顶层设计，明确密码应用需求和预期目标，并与本平台网络安全保护等级相结合，通过成体系的设计形成涵盖技术、管理、实施保障的整体方案，为落实密码应用相关要求奠定基础。

（2）**完备性原则**。围绕本平台实际业务应用与安全保护等级，站在整体角度，通过自上而下的体系化设计，综合考虑物理和环境安全、网络和通信安全、设备和计算安全、应用和数据安全等多个层面密码应用需求，设计密码应用方案。

（3）**经济性原则**。结合本平台规模，在合理、够用的前提下，设计满足GB/T 39786-2021《信息安全技术 信息系统密码应用基本要求》的密码应用方案，确保本期项目的密码应用投资合理，规模适度，避免资金浪费和过度保护。

**4.2.2 主要依据**

* 《中华人民共和国网络安全法》
* 《中华人民共和国密码法》
* 《中华人民共和国电子签名法》
* 《关键信息基础设施安全保护条例》
* 《网络安全等级保护条例（征求意见稿）》
* 《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》
* 《国家政务信息化项目建设管理办法》（国办发【2019】57号）
* GB/T 39786-2021 信息安全技术 信息系统密码应用基本要求
* GM/T 0014-2012《证书认证系统密码协议规范》
* 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 0027-2014《智能密码钥匙技术规范》
* GM/T 0028-2014《密码模块安全技术要求》
* GM/T 0030-2014《密码机技术规范》
* GM/T 0034-2014《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 0036-2014《采用非接触卡的门禁系统密码应用技术指南》
* GM/T 0041-2015《智能IC卡密码检测规范》
* GM/T 0115-2021 信息系统密码应用测评要求
* GM/T 0116-2021 信息系统密码应用测评过程指南
* GB/T 35276-2017《信息安全技术 SM2 密码算法使用规范》
* GB/T 32905-2016《信息安全技术 SM3 密码杂凑算法》
* GB/T 32907-2016《信息安全技术 SM4 分组密码算法》
* GB/T 35291-2017 《信息安全技术 智能密码钥匙应用接口规范》
* GM/T 0063-2018 《智能密码钥匙密码应用接口检测规范》
* GB/T 36322-2018 《信息安全技术 密码设备应用接口规范》
* GB/T 37092-2018 《信息安全技术 密码模块安全要求》
* 《信息系统密码应用高风险判定指引》
* 《商用密码应用安全性评估管理办法（试行）》
* 《商用密码应用安全性评估量化评估规则》

**5 总体设计方案**

本系统为新建系统，已采购国密的SSL VPN安全网关、服务器密码机、国密身份认证系统、传输透明加密系统、UKey、数字证书等来建立网络和通信层面、应用和数据层面的部分指标项的密码安全。

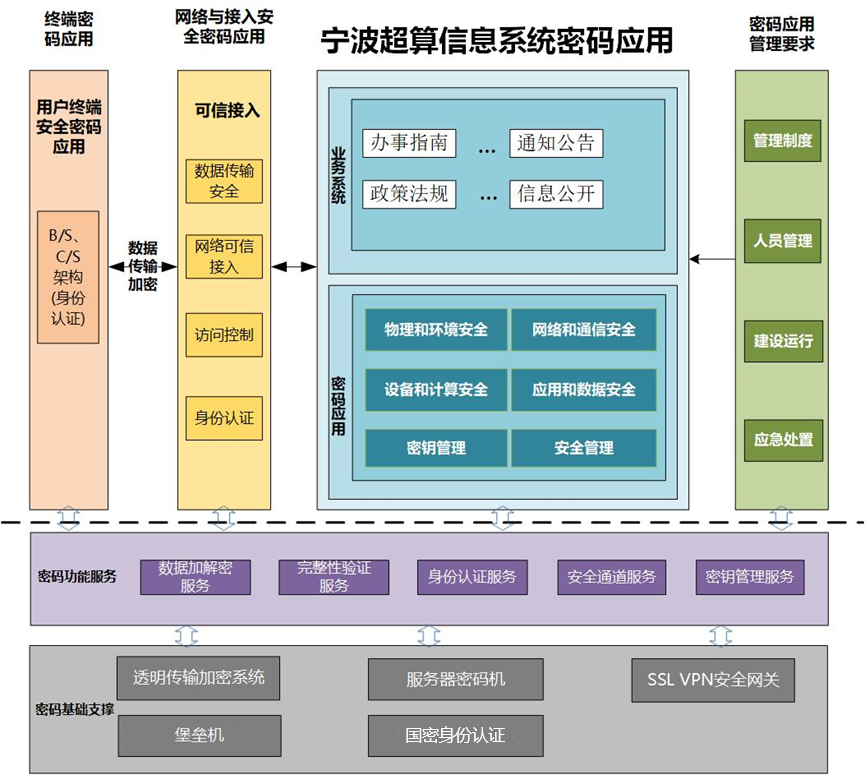


图5-1 XX人工智能超算中心HPC超级计算集群系统密码应用技术框架

其中：

**1）SSL VPN安全网关**：主要用于在网络上建立安全的信息传输通道，通过对数据包的加密和数据包目标地址的转换实现远程访问，进行加密通信。

**2）服务器密码机**：实现数据加密、数字签名、随机数生成等功能，保证数据的机密性、完整性。

**3）传输透明加密系统：**系统采用标准国密SM4分组对称加密算法、SM2椭圆曲线公钥密码算法和SM3密码杂凑算法。可为多种操作系统的浏览器终端提供身份认证、加密通信、完整性保护服务。

**4）国密身份认证系统：**基于密钥分割技术和协同签名技术，实现密钥分量在用户终端和服务端独立生成和独立存储。采用国密算法，为浏览器终端提供身份认证服务。

**5）智能密码钥匙**：具备数字证书，采用国密SM2算法实现身份鉴别。

**6 详细方案设计**

**6.1 物理和环境安全**

### 6.1.1 总体要求

物理和环境安全总体要求应采用密码技术对重要场所、监控设备等物理访问进行控制；采用密码技术对物理访问控制记录、监控信息等物理和环境的敏感信息数据实施完整性保护；基于总体要求采用数据完整性保护机制保证访问控制记录、监控信息等物理环境的敏感信息的完整性。

### 6.1.2 功能设计

在本平台所在的本地机房区域部署符合GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》的安全门禁系统，使用SM1算法进行密钥分散，实现门禁卡的“一卡一密”，并基于SM1算法对人员身份进行鉴别；使用SM2数字签名技术对门禁进出记录进行完整性保护；

在本平台使用符合密码相关国家、行业标准要求的国密音视频监控系统，使用HMAC-SM3对视频监控系统视频记录数据进行完整性保护。

物理和环境安全层面使用的密码算法、密码技术、密钥管理由符合GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》、GM/T 0028-2014《密码模块安全技术要求》的电子门禁系统及符合密码相关国家、行业标准要求的国密音视频监控系统实现。

视频监控安全管理系统业务主要包括门禁系统和视频监控系统两大系统，和提供安全管理支撑的安全管理子系统。其通过管理符合国密标准的门禁设备和视频设备，实现物理身份鉴别、门禁记录完整性和视频记录完整性的保护。

其系统部署架构如下图所示：

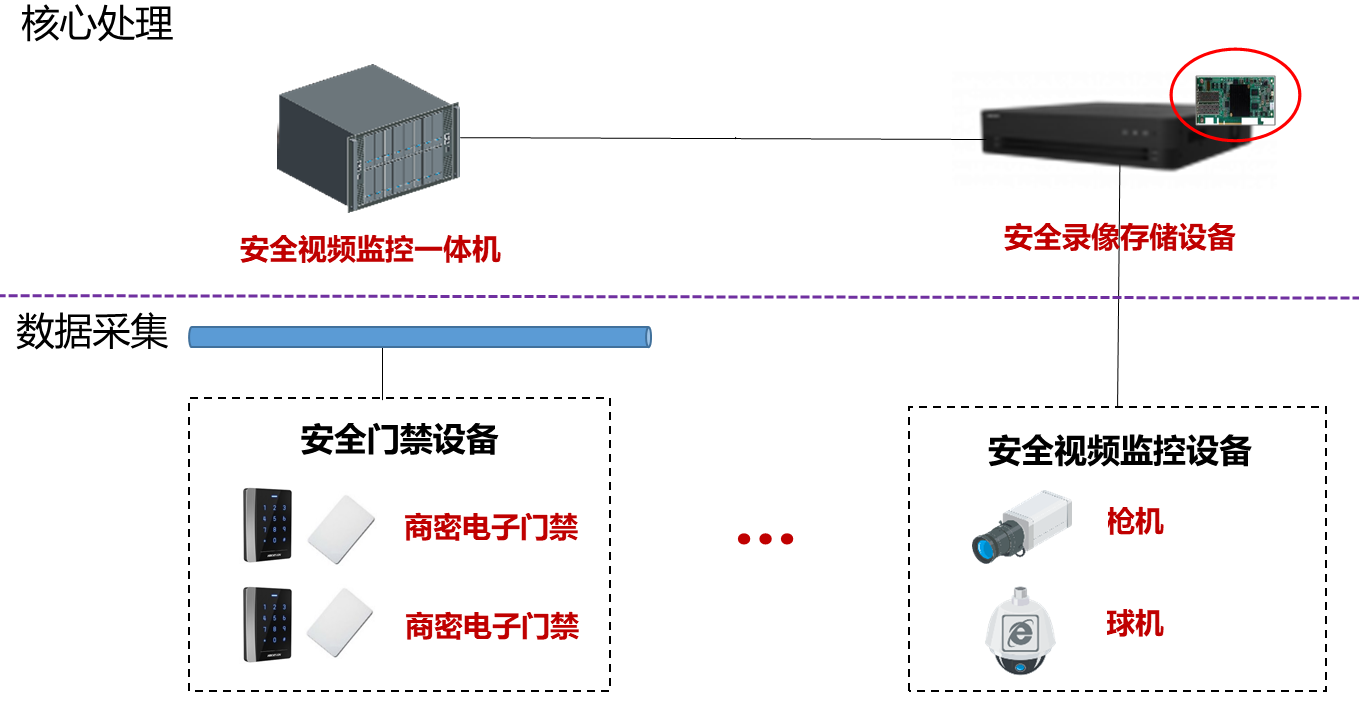


图6-1 系统部署架构图

（1）物理身份鉴别

门禁子系统的访问使用国密CPU卡进行物理因子的身份认证机制（排除人脸、指纹和口令的不可靠性），CPU卡要求通过国家密码管理局检测认证，具备相关国密证书。

管理系统采用口令+USBKey的双因素身份认证机制，保证系统访问的可靠性。USBKey要求通过国家密码管理局检测认证，具备相关国密证书。

（2）门禁记录完整性保护

门禁读卡器触发国密CPU卡刷卡记录时，上报到门禁子系统，系统会记录本条门禁刷卡记录信息（信息包含卡片ID、门禁事件类型、事件内容、事件结果、事件时间等）。同时，系统调用内置密码模块对该条门禁记录进行签名，并将该记录和签名结果保存到数据库中，实现门禁记录存储的完整性保护。

安全审计员进入系统后，可查询门禁记录信息，并对门禁记录进行审计管理，审计时可调用签名公钥对签名结果进行验签，若验签失败则记录审计失败。同时，该审计结果也将用该审计员私钥签名并记录在数据中，保证其审计结果的不可否认性。



图6-2 门禁记录完整性保护

（3）视频记录完整性保护

视频存储服务器在接收到视频数据时会先进行数据分片并作冗余处理（用于数据损坏恢复），分片处理完成后会对其整个数据分片进行签名处理并保存签名结果。同时，在视频记录被调用时，会对其进行验签，校验其完整性，判断其是否被非法篡改。



图6-3 视频记录完整性保护

**6.2 网络和通信安全**

### 6.2.1 总体要求

网络和通信安全的总体要求总则：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；采用密码技术保证通信过程中数据的完整性;采用密码技术保证通信过程中敏感信息数据字段或整个报文的机密性；在互联网出口区采用密码技术保证网络边界访问控制信；采用密码技术建立一条安全的信息传输通道，对网络中的安全设备或安全组件进行集中管理。

### 6.2.2 功能设计

（1）业务通道：

采用合规机构签发的数字证书、配合Https协议建立安全传输通道，业务用户通过非国密浏览器访问登录应用系统，系统采用RSA2048算法实现客户端与服务端通信实体的身份鉴别，采用AES256算法实现通信过程中数据的机密性、完整性保护。

（2）运维管理通道：

设备运维人员可以通过互联网登录SSL VPN客户端访问登录SSL VPN安全网关后通过堡垒机对设备进行统一运维。SSL VPN安全网关采用基于国产密码算法（SM2、SM3、SM4）的SSL协议进行通信，实现对通信双方进行身份鉴别（SM2算法），通信数据完整性（HMMA-SM3算法），通信过程中重要数据的机密性（SM4算法）。

**6.3 设备和计算安全**

### 6.3.1 总体要求

设备与计算安全需采用密码技术对登录的用户进行身份鉴别，在本系统业务区PC端部署安全浏览器，对登录设备（堡垒机、VPN等设备）的用户进行身份鉴别，防止非授权人员登录、管理员远程登录身份鉴别信息被非授权窃取。

对设备的远程操作管理通过SSL VPN网关等设备，建立安全的信息传输通道，实现管理过程中通信的机密性、完整性。

### 6.3.2 功能设计

（1）身份鉴别及管理通道安全

基于超算集群系统中密码基础设备底座为:SSL VPN安全网关，采用基于国产密码算法（SM2、SM3、SM4）的SSL协议进行通信，向本平台设备管理员配发数字证书的USB key，基于SM2算法进行身份鉴别。通过防火墙及SSL VPN网关的访问控制列表方式限制堡垒机为运维接入人员访问的唯一目的地址，并通过登录堡垒机对应用服务器、数据库服务器、数据库管理系统进行统一的运维管理。

（2）访问控制信息安全

信息系统中密码设备都具有商用密码产品认证证书，达到GB/T 37092二级及以上安全要求，故密码设备采用自身的安全机制实现访问控制信息安全保护。系统所涉及的非密码产品，如应用服务器、数据库等通用设备，需借助外部密码产品且需开放设备底层资源才可完成相关建设；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。对设备管理员进行详细的权限管理，遵循权限分离原则，只分配给管理员完成操作所需的最小权限，通过严格的管理措施降低安全风险。

（3）重要信息资源信息安全标记

各类物理设备等系统资源的访问控制信息、重要信息资源安全标记、日志记录等，在OS存储过程中结合HMAC或数字签名等密码技术实现完整性保护，防止重要资源数据被恶意篡改。

（4）日志记录完整性保护

信息系统中密码设备都具有商用密码产品认证证书，达到GB/T 37092二级及以上安全要求，故密码设备采用自身的安全机制实现对密码设备日志记录完整性保护，同时平台对设备收集的日志信息通过HMAC-SM3保护日志完整性，HMAC-SM3基于应用层内置密码模块实现，密码模块对接硬件服务密码机。

（5）重要可执行程序安全

系统所涉及的非密码产品，如应用服务器、数据库等通用设备，需借助外部密码产品且需开放设备底层资源才可完成相关建设；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。

系统中重要可执行程序均从官方渠道获取，且在安装前对程序进行验证，保证其没有受到篡改，在一定程度上降低重要可执行程序完整性、重要可执行程序来源真实性保护的安全风险，不做改造。

信息系统中密码设备都具有商用密码产品认证证书，达到GB/T 37092二级及以上安全要求，故密码设备采用自身的安全机制实现密码设备重要可执行程序完整性、重要可执行程序来源真实性。

**6.4 应用和数据安全**

### 6.4.1 总体要求

利用USB Key、统一身份认证系统等满足应用系统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的需求。

利用服务器密码机等设备对用户注册信息（个人姓名、手机号码、单位信息）、身份鉴别信息、访问控制信息、重要日志等重要数据进行数据传输及存储过程中的机密性、完整性保护。

### 6.4.2 功能设计

1. 登录用户身份的真实性

在本系统所在的本地机房部署符合密码相关国家、行业标准要求的国密身份认证系统，系统账号权限同步至国密身份认证系统产品，本平台系统管理员，普通用户通过PC端浏览器采用国密身份认证系统提供的智能密码钥匙使用国密SM2算法采用密码技术验证的方式进行登录。

（2）重要信息资源安全标记的完整性

各类物理设备等系统资源的访问控制信息、重要信息资源安全标记、日志记录等，在OS存储过程中结合HMAC或数字签名等密码技术实现完整性保护，防止重要资源数据被恶意篡改。

（3）访问控制信息的完整性

在本系统所在的本地机房部署符合密码相关国家、行业标准的服务器密码机，采用HMAC-SM3技术对应用访问控制信息进行实现信息完整性保护，防止应用资源被非授权访问。

（4）传输机密性、完整性保护

在本系统内核心机房的安全管理区部署符合密码相关国家、行业标准要求的传输透明加密系统，基于传输加密技术，以轻量级改造的方式，实现Web/H5应用的传输加密，用户终端动态加载加解密算法模块，实现数据在浏览器页面加密，采用SM4算法对本平台中用户注册信息（个人姓名、手机号码、单位信息、账号口令）等进行机密性保护，实现重要数据防窃取保护。

采用HMAC-SM3算法对本平台中用户注册信息（个人姓名、手机号码、单位信息、账号口令）等进行传输完整性保护，实现重要数据防篡改保护。

（5）存储机密性、完整性保护

本系统所在的本地机房部署符合密码相关国家、行业标准的服务器密码机，采用SM4-CBC算法实现用户注册信息（个人姓名、手机号码、单位信息、账号口令）进行机密性保护。并使用HMAC-SM3算法对用户注册信息（个人姓名、手机号码、单位信息、账号口令）、日志数据等重要数据进行完整性保护。

（6）不可否认性保护

本系统不涉及电子商务、CA认证、网上银行、证券交易、电子合同、电子公文等（可能涉及法律责任认定的应用），目前没有不可否认性保护需求，故无需部署相关密码产品。

**6.5 密钥管理安全**

本平台使用的数字证书由CA机构颁发。本平台会严格遵照制定的管理操作规程，保证密钥等信息和系统的部署、使用安全。

应用和数据层面拥有完善的密钥管理体系，其中密钥管理系统需要安装在硬件服务器中，为信息系统提供加解密、完整性保护和身份认证服务。

**6.5.1 国密身份认证系统**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **密钥产生** | **密钥分发** | **密钥存储** | **密钥使用** | **密钥更新** | **密钥归档** | **密钥撤销** | **密钥备份** | **密钥恢复** | **密钥销毁** |
| 1 | SM2公钥 | 初始化将签名证书导入加密卡中、由加密卡进行产生 | 客户端请求服务端获取公钥 | 存储在pcie加密卡中 | 用于D2验签 | 无更新需求 | 无归档需求 | 导入新的证书到加密卡中，生成新的公私钥对，原有sm2密钥会失效 | 加密卡中的密钥信息备份到加密卡中的ukey | 将备份的二进制文件重新导入到加密卡中 | 使用完后，对所在内存块进行memset全零覆盖处理 |
| 2 | SM2私钥 | 初始化将签名证书导入加密卡中、由加密卡进行产生 | 不进行分发 | 存储在pcie加密卡中 | 用于对D2分量密钥进行签名 | 无更新需求 | 无归档需求 | 导入新的证书到加密卡中，生成新的公私钥对，原有sm2密钥会失效 | 加密卡中的密钥信息备份到加密卡中的ukey | 将备份的二进制文件重新导入到加密卡中 | 使用完后，对所在内存块进行memset全零覆盖处理 |
| 3 | SM4密钥 | Ueky初始化时，调用ukey随机数接口生成32字节随机数作为sm4密钥 | 不进行分发 | 存储在ukey中 | 用于写入ukey中用户数据进行加解密 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 重新初始化后销毁 |
| 4 | 会话密钥 | 调用随机数生成接口生成32字节随机数作为会话密钥 | 通过获取的sm2公钥，将密钥加密发送到服务端 | 存储在内存中 | 用于用户在协同签名时，对数据进行加解密 ，一次一密 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 通信过程连接断开时进行销毁 |
| 4 | 私钥分量D1 | 调用ueky随机数接口生成32字节随机数作为私钥分量D1 | 不进行分发 | 存储在ukey中 | 用于用户在协同签名时，产生私钥分量D2所需的P1 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 重新初始化ukey销毁 |
| 5 | 私钥分量D2 | 根据D1的P1产生 | 不进行分发 | 存储在服务端数据库中 | 用于用户在协同签名时，进行签名 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | Ueky初始化后对数据库该记录销毁 |

**6.5.2 SSL VPN安全网关密钥管理**

根证书存储在SSL VPN网关设备中进行管理，私钥存储在USB Key中，实现登录业务系统用户的身份鉴别服务，保障登录用户身份的真实性。

（1）密钥体系

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 序号 | 密钥种类 | 功能 | 更新 | 备份 |
| 1 | 设备密钥 | 保护服务端密（签名密钥、加密密钥）钥、密钥加密密钥的安全 | 不支持 | 不支持 |
| 2 | 服务端密密钥 | 服务端加密密钥用于SSL握手过程中预主密钥的协商、加密系统配置信息；  服务端签名密钥用于SSL握手过程中服务端身份鉴别 | 不支持 | 支持 |
| 3 | 预主密钥 | 用于生成主密钥 | 不支持 | 不支持 |
| 4 | 主密钥 | 用于生成工作密钥 | 不支持 | 不支持 |
| 5 | 工作密钥 | 加密密钥用于数据加解密校验密钥用于数据校验 | 支持 | 不支持 |
| 6 | 密钥加密密钥 | 用于保护工作密钥 | 不支持 | 支持 |
| 7 | 配置数据校验密钥 | 用于配置数据校验 | 不支持 | 不支 |
| 8 | 会话密钥 | 管理员登录认证过程中对数据进行加密 | 不支持 | 不支持 |

（2）密钥全生命周期

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 安全参数 | 生成 | 导入/导出 | 存储 | 使用 | 更新 | 销毁/  置零 | 备份 |
| 设备密钥 | 调用密码卡随机数生成器生成真随机数作为设备密钥 | 不支持 | 存储在密码卡内存安全存储区域， | 保护服务端密密钥的安全。 | 不支持 | 恢复出厂设置 | 在本系统中没有备份。 |
| 服务端密密钥 | 1、服务端签名密钥对由密码卡SM2密钥对，并将公钥导出，打包成证，申请CA签发设备身份证书；  2、服务端加密密钥对通过CA中心加密下发 | 只有公钥可以导出；  加密密钥对以密文形式导入 | 使用设备主密钥加密存储在密码卡内部易非失性存储区。 | 1、服务端加密密钥用于SSL握手过程中预主密钥的协商、加密系统配置信息；  2、服务端签名密钥用于SSL握手过程中服务端身份鉴别；  3、管理员登录认证过程中使用服务端加密密钥公钥加密会话密钥，服务端使用服务端加密密钥私钥解密出会话密钥。 | 不支持 | 调用密码卡密钥销毁接口对将密码卡内密钥进行全零覆盖销毁。无法恢复 | 管理员使用密钥管理工具加密备份到文件中。 |
| 预主密钥 | 由客户端调用硬件随机数接口生成随机数作为预主密钥。 | 由客户端使用服务端密钥中的加密密钥公钥进行加密传输给服务端 | 不存储，每次密钥协商时生成新的预主密钥 | 用于生成主密钥 | 不支持 | 生成主密钥后对密文预主密钥以及解密后的明文预主密钥进行置零销毁 | 不支持 |
| 主密钥 | 由预主密钥、客户端随机数、服务端随机数、常量字符经过计算生成。 | 不支持 | 不存储，每次密钥协商时生成新的主密钥 | 用于生成工作密钥 | 不支持 | 生成工作密钥后对主密钥进行置零销毁 | 不支持 |
| 工作密钥 | 加密密钥由预主密钥、客户端随机数、服务端随机数、常量字符经过计算生成；  校验密钥由预主密钥、客户端随机数、服务端随机数、常量字符经过计算生成。 | 不支持 | 使用密钥加密密钥加密后存储在密码卡易失性存储区。 | 加密密钥用于数据加解密。校验密钥用于数据校验 | 在设置的密钥更新周期时间到达时，密码模块自动进行新的密钥交换参数协商，  ，密钥交换参数协商完成后时由主密钥、客户端随机数、服务端随机数、常量字符经过计算生成新的工作密钥。 | 密钥更新时对旧的工作密钥进行销毁置零操作，密码卡恢复出厂设置时易失性存储区内的工作密钥被销毁无法恢复。连接断开时对连接所属的工作密钥进行置零处理，设备断电后易失性存储区恢复至初始状态，密钥被清除无法被恢复。 | 不支持 |
| 密钥加密密钥 | 设备初始化时调用密码卡接口生成真随机数作为密钥加密密钥。 | 不支持 | 使设备密钥加密存储在密码卡内部易非失性存储区。 | 用于保护工作密钥。 | 不支持。 | 恢复出厂时，通过调用密码卡密钥销毁接口对密钥进行memset全零覆盖销毁，无法重新恢复。 | 管理员使用密钥管理工具加密备份到文件中。 |
| 配置数据校验密钥 | 模块初始化时调用密码卡随机数生成器生成真随机数作为配置数据校验密钥 | 不支持 | 使用服务端密钥中的加密密钥加密存储在密码卡内非易失性存储区。 | 用于配置数据校验。 | 不支持 | 恢复出厂时，通过调用密码卡密钥销毁接口对密钥进行memset全零覆盖销毁，无法重新恢复。 | 不支持。 |
| 会话密钥 | 管理员登录认证时调用随机数生成接口生成真随机数作为会话密钥。 | 不支持。 | 一次一密，不进行存储。 | 管理员登录认证过程中对数据进行加密。 | 不支持。 | 使用完后，对所在内存块进行memset全零覆盖处理。 | 不支持。 |

**6.5.3 传输透明加密系统**

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **密钥产生** | **密钥分发** | **密钥存储** | **密钥使用** | **密钥更新** | **密钥归档** | **密钥撤销** | **密钥备份** | **密钥恢复** | **密钥销毁** |
| 1 | SM2公钥 | 初始化将签名证书导入加密卡中、由加密卡进行产生 | 客户端请求服务端获取公钥 | 存储在pcie加密卡中 | 用于对验签 | 无更新需求 | 无归档需求 | 导入新的证书到加密卡中，生成新的公私钥对，原有sm2密钥会失效 | 加密卡中的密钥信息备份到加密卡中的ukey | 将备份的二进制文件重新导入到加密卡中 | 使用完后，对所在内存块进行memset全零覆盖处理 |
| 2 | SM2私钥 | 初始化将签名证书导入加密卡中、由加密卡进行产生 | 不进行分发 | 存储在pcie加密卡中 | 用于对SM4密钥进行签名 | 无更新需求 | 无归档需求 | 导入新的证书到加密卡中，生成新的公私钥对，原有sm2密钥会失效 | 加密卡中的密钥信息备份到加密卡中的ukey | 将备份的二进制文件重新导入到加密卡中 | 使用完后，对所在内存块进行memset全零覆盖处理 |
| 3 | SM4密钥 | 调用密码卡随机数生成接口生成32字节随机数作为sm4密钥。 | 通过协同签名后，将密钥发送给客户端 | 存储在pcie加密卡中 | 用于用户通信过程中对业务数据进行加解密 ，一次一密 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 通信过程连接断开时进行销毁 |
| 4 | 会话密钥 | 调用随机数生成接口生成32字节随机数作为会话密钥 | 通过获取的sm2公钥，将密钥加密发送到服务端 | 存储在内存中 | 用于用户在协同签名时，对数据进行加解密 ，一次一密 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 通信过程连接断开时进行销毁 |
| 5 | 私钥分量D1 | 调用随机数生成接口生成32字节随机数作为私钥分量D1 | 不进行分发 | 存储在内存中 | 用于用户在协同签名时，产生私钥分量D2所需的P1 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 通信过程连接断开时进行销毁 |
| 6 | 私钥分量D2 | 调用客户端发送的P1产生 | 不进行分发 | 存储在内存中 | 用于用户在协同签名时，进行签名 | 无更新需求 | 无归档需求 | 无撤销需求 | 无备份需求 | 无恢复需求 | 通信过程连接断开时进行销毁 |

**6.5.4 服务器密码机密码密钥管理**

| 密钥名称 | 密钥生成/导入 | 密钥导出 | 密钥存储 | 密钥使用 | 密钥更新 | 密钥销毁 | 密钥备份 |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 设备主密钥 | 由密码卡初始化时调用随机数生成接口生成真随机数作为设备主密钥。 | 不可导出 | 设备主密钥分2部分存储，一部分储存在密码卡内，一部分加密存储在管理员UKEY内 | 保护密码机内存储的设备密钥、用户密钥和密钥加密密钥的存储安全 | 不支持 | 可以通过密钥销毁锁进行紧急密钥销毁 | 不支持 |
| 设备密钥 | 设备签名密钥对由密钥卡初始化时调用SM2算法模块随机生成一对密钥作为设备签名密钥对并加密存储在密码卡0号索引位置； 设备加密密钥对由CA中心加密导入到密码机中并存储在密码机0号索引位置 | 只有公钥能导出 | 使用设备主密钥进行SM1算法加密后存储在密码卡安全存储区域。 | 设备签名密钥对用于密码机身份认证； 设备加密密钥对用于会话密钥协商和敏感数据加密 | 不支持 | 可以通过密钥销毁锁进行紧急密钥销毁 | 可以通过密码机管理客户端将设备密钥以密文文件形式备份到本地 |
| 用户密钥 | 用户签名密钥对通过调用SM2算法模块随机生成一对密钥对存储到密码卡指定索引位置； 设备加密密钥对由CA中心加密导入到密码机中并存储在密码机指定索引位置 | 只有公钥能导出 | 使用设备主密钥进行SM1算法加密后存储在密码卡安全存储区域。 | 签名密钥对用于用户身份认证；加密密钥对用于业务系统会话密钥协商和敏感数据加密 | 可通过管理客户端工具对指定索引的密钥进行删除并重新生成新的密钥 | 可以通过管理客户端删除指定索引的密钥或通过密钥销毁锁进行紧急密钥销毁 | 可以通过密码机管理客户端将用户密钥以密文文件形式备份到本地 |
| 密钥加密密钥 | 调用密码卡随机数生成接口生成真随机数存储到密码卡指定索引存储位置。 | 无法导出。 | 使用设备主密钥进行SM1算法加密后存储在密码卡安全存储区域。 | 用于会话密钥加密保护 | 可通过管理客户端工具对指定索引的密钥进行删除并重新生成新的密钥 | 可以通过管理客户端删除指定索引的密钥或通过密钥销毁锁进行紧急密钥销毁 | 可以通过密码机管理客户端将密钥加密密钥以密文文件形式备份到本地 |
| 会话密钥 | 调用密码卡随机数生成接口生成真随机数作为会话密钥。 | 不支持（密钥分发：可以通过设备密钥、用户密钥和密钥加密密钥加密分发到通信对端） | 即用即销毁。一次一密 | 用于会话过程中的业务数据进行加密并计算业务数据的MAC值。 | 不支持 | 每次会话结束时销毁。一次一密。 | 不支持 |

**6.6 密码应用流程**

**6.6.1 国密身份认证流程**



图6-4 国密身份认证时序图

**6.6.2 SSL VPN安全网关管理流程**

针对于远程运维场景，采用SSL VPN安全网关，结合含有数字证书的USBKey，实现远程运维管理终端与系统之间的运维人员身份鉴别、数据传输的机密性与完整性保护。

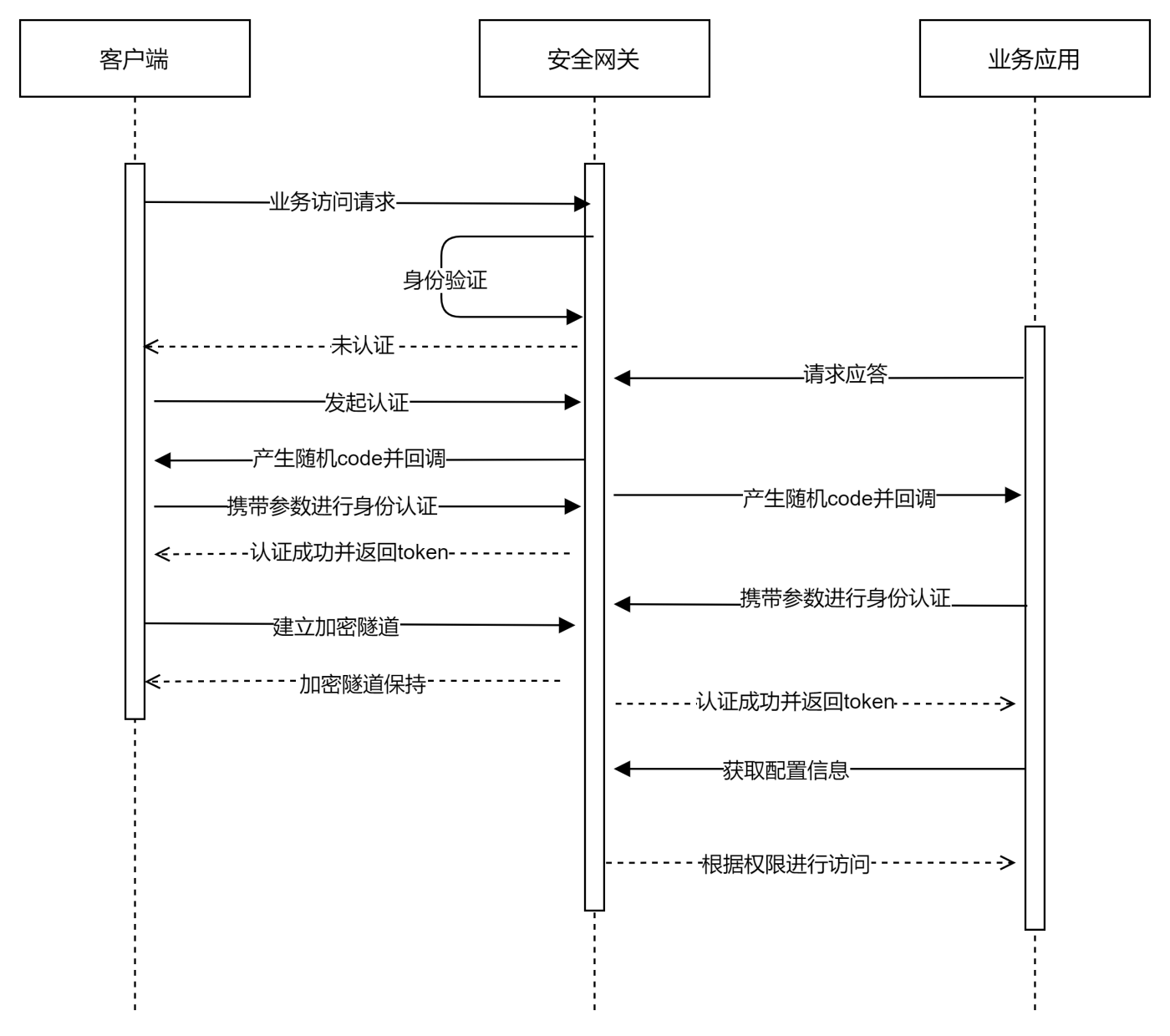


图6-5 安全网关交互时序图

**6.6.3 传输透明加密系统流程说明**

传输透明加密系统对Web页面注入可加载的算法模块。算法模块首先基于协同签名系统技术对登录事件做客户端身份认证，再进行数据拦截并国密加密，密文传输至DMZ隔离区域，最终在传输透明加密系统服务器解密转发，在内部可信环境下明文办公。具体流程如下：

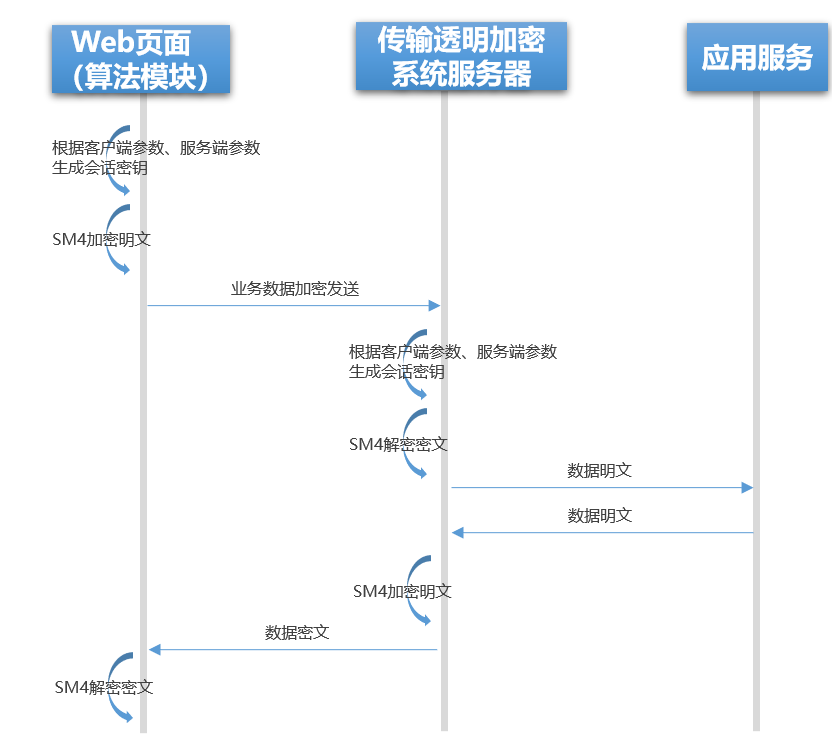


图6-6 传输透明加密系统功能流程说明

**6.6.4 服务器密码机流程说明**

系统中的应用服务器通过集成服务器密码机接口，数据需要进行加解密过程时通过调用已集成的SDK，将数据进行加解密操作以及完整性校验工作。具体流程如下：

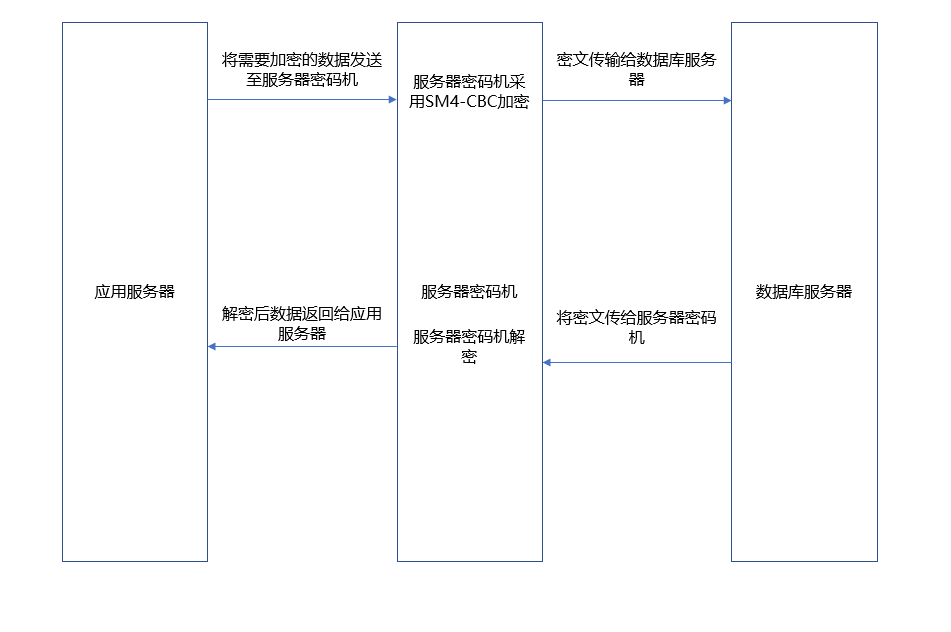


图6-7 服务器密码机机密性功能流程说明

* 服务器密码机加密过程简要流程说明：

1. 应用服务器通过调用已集成的服务器密码机接口，将数据明文传输至服务器密码机处。
2. 服务器密码机基于SM4算法，使用密钥实现数据加密，实现数据的机密性保护，保证数据不被泄露给非授权的实体。
3. 服务器密码机通过接口的方式将数据密文传输至应用服务器侧进行密文存储。

* 服务器密码机解密简要流程说明

1. 应用服务器通过调用接口，将密文数据传输至服务器密码机处。
2. 服务器密码机基于SM4算法，使用密钥对数据解密，得到对应的明文数据。
3. 服务器密码机通过接口的方式将数据明文传输至应用服务器侧，完成数据解密过程。

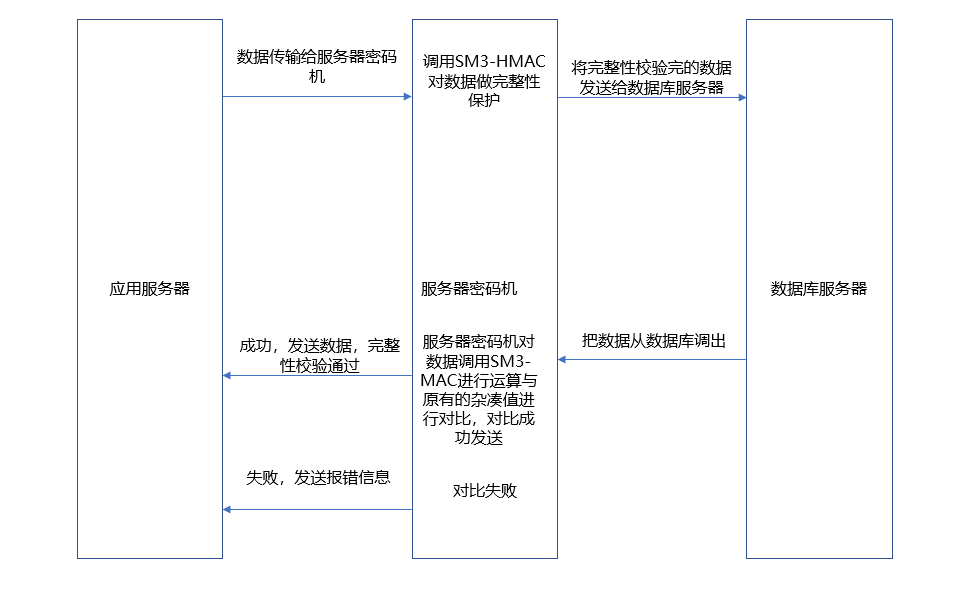


图6-8 服务器密码机完整性功能流程说明

* 服务器密码机完整性加密简要说明：

1. 应用服务器通过调用已集成的服务器密码机接口，将数据明文传输至服务器密码机处。
2. 服务器密码机基于HMAC-SM3算法，使用密钥实现数据加密，得到对应的HMAC值。
3. 服务器密码机通过接口的方式将HMAC值传输至应用服务器侧进行密文存储。

* 服务器密码机完整性校验简要说明：
* 应用服务器通过调用接口，将当前重要数据关键信息以及最近一次关键信息的MAC值推送至服务器密码机，申请MAC校验。
* 服务器密码机获取当前重要数据的相关关键信息，以及最近一次关键信息的MAC值。
* 服务器密码机使用SM3杂凑算法，计算当前重要数据的相关关键信息及系统密钥的MAC值。
* 服务器密码机比较当前重要数据的相关关键信息和最近一次重要数据的相关关键信息的MAC值，是否一致，并向系统返回结果（如果两个MAC值一致，说明当前重要数据未被篡改，系统根据用户需要推送重要数据；如果两个MAC值不一致，说明当前重要数据已经被篡改，系统通知系统管理人员处理）

**6.7 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 | 采取措施 | 标准符合性（符合**/**部分符合**/**不符合**/**不适用） | 说明（针对不适用项说明原因及替代性措施） |
| --- | --- | --- | --- | --- |
| 物理和环境安全 | 身份鉴别 | 在本平台所在的本地机房区域部署符合GM/T 0036-2014《采用非接触卡的门禁系统密码应用指南》的安全门禁系统，门禁卡+电子门禁系统，使用SM1算法进行密钥分散，实现门禁卡的“一卡一密”，并基于SM1算法对人员身份进行鉴别；使用SM2数字签名技术对门禁进出记录进行完整性保护。 | 符合 | 无 |
| 电子门禁记录数据完整性 |
| 视频监控记录数据存储完整性 | 在本平台所在的本地机房使用国密视频监控系统，实现对视频监控数据的完整性（HMAC-SM3算法）保护。 |
| 网络和通信安全 | 身份鉴别 | 业务通道：采用RSA2048算法实现通信实体的身份鉴别。 | 符合 | 无 |
| 运维通道： USB Key+国密SSL VPN网关设备实现远端运维人员身份鉴别。 | 符合 |
| 通信数据完整性 | 业务通道：AES256算法实现通信数据的完整性保护。 | 符合 |
| 运维通道：USB Key+国密SSL VPN网关设备实现远端运维通信数据的完整性保护。 | 符合 |
| 通信过程中重要数据的机密性 | 采用AES256算法实现通信过程中重要数据的机密性保护。 | 符合 |
| 运维通道： USB Key+国密SSL VPN网关设备实现远端运维通信数据的机密性保护。 | 符合 |
| 网络边界访问控制信息完整性 | USB Key+国密SSL VPN网关设备，对通信双方进行身份鉴别，利用HMAC-SM3算法对访问控制信息进行完整性、机密性保护，建立基于密码算法的数据加密传输通道。 | 部分符合 |
| 安全接入认证 | 1、业务通道：  采用合规机构签发的数字证书、配合Https协议建立安全传输通道，系统采用RSA2048算法实现客户端与服务端通信实体的身份鉴别，采用AES256算法实现通信过程中数据的机密性、完整性保护。  2、运维管理通道：  设备运维人员可以通过互联网登录SSL VPN客户端访问登录SSL VPN安全网关后通过堡垒机对设备进行统一运维。SSL VPN安全网关采用基于国产密码算法（SM2、SM3、SM4）的SSL协议进行通信，实现对通信双方进行身份鉴别（SM2算法），通信数据完整性（HMMA-SM3算法），通信过程中重要数据的机密性（SM4算法）。 | 符合 | 无 |
| 设备和计算安全 | 身份鉴别 | 向本平台管理员配发USB接口的智能密码钥匙（USBKey），结合SSL VPN安全网关，并将已部署的SSL VPN安全网关与堡垒机进行对接，限制堡垒机为各个设备登录的唯一源地址，实现对系统管理员进行身份鉴别和远程管理身份鉴别信息传输机密性保护，防止非授权人员登录。以保证在远程管理时实现信息、数据的防窃听。 | 部分符合 | 除堡垒机、SSL VPN安全网关外，其余应用服务器、数据库服务器、数据库管理系统等各类设备暂无法实现身份鉴别，通过堡垒机进行统一运维管理降低风险。 |
| 远程管理通道安全 | 基于超算集群系统中的安全通道服务能力（密码基础设备底座为:SSL VPN安全网关），并将部署的SSL VPN安全网关与堡垒机进行对接，限制堡垒机为各个设备登录的唯一源地址以建立安全的数据传输通道，（采用基于国产密码算法（SM2、SM3、SM4）的SSL协议进行通信）保护传输过程中数据的机密性和完整性。 | 部分符合 | 除堡垒机、SSL VPN安全网关外，其余应用服务器、数据库服务器、数据库管理系统等各类设备暂无法实现远程管理通信的安全，通过堡垒机进行统一运维管理降低风险。 |
| 重要信息资源安全标记完整性 | 各类物理设备等系统资源的访问控制信息、重要信息资源安全标记、日志记录等，在OS存储过程中结合HMAC或数字签名等密码技术实现完整性保护，防止重要资源数据被恶意篡改。 | 符合 | 无 |
| 访问控制信息完整性 | 在本系统所在的本地机房部署符合密码相关国家、行业标准的服务器密码机，采用HMAC-SM3技术对应用访问控制信息进行实现信息完整性保护，防止应用资源被非授权访问。 | 符合 | 无 |
| 日志记录完整性 | 审计服务记录用户登录等操作事件时，将审计事件的重要数据拼接后计算HAMC值（基于商密算法ALG\_HMAC\_SM3计算的HMAC值），与日志数据保存于数据库中，用户在查询审计事件时校验审计事件是否被篡改。 | 符合 | 无 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 系统中重要可执行程序均从官方渠道获取，且在安装前对程序进行验证，保证其没有受到篡改，在一定程度上降低重要可执行程序完整性、重要可执行程序来源真实性保护的安全风险。 | 部分符合 | 无 |
| 应用和数据安全 | 身份鉴别 | B/S架构身份鉴别  互联网场景：在本系统所在的本地机房部署符合密码相关国家、行业标准要求的国密身份认证系统，采用智能密码钥匙进行身份鉴别。 | 符合 | 无 |
| 访问控制信息完整性 | 本系统所在的本地机房部署符合密码相关国家、行业标准的服务器密码机，采用HMAC-SM3技术对应用访问控制信息进行实现信息完整性保护，防止应用资源被非授权访问。 | 符合 | 无 |
| 重要数据传输机密性 | 在本系统内核心机房的安全管理区部署符合密码相关国家、行业标准要求的传输透明加密系统，采用密码设备提供的传输加密服务，基于传输加密技术，以轻量级改造的方式，实现Web/H5应用的传输加密，用户终端动态加载加解密算法模块，实现数据在浏览器页面加密，对用户身份鉴别数据、重要业务数据等关键数据进行传输机密性、完整性保护，实现身份鉴别数据、重要业务数据防窃取和防篡改保护。 | 符合 | 无 |
| 重要数据传输完整性 | 符合 | 无 |
| 重要数据存储机密性 | 本系统所在的本地机房部署符合密码相关国家、行业标准的服务器密码机，采用SM4-CBC算法实现用户注册信息（个人姓名、手机号码、单位信息、账号口令）进行机密性保护。并使用HMAC-SM3算法对用户注册信息（个人姓名、手机号码、单位信息、账号口令）、日志数据等重要数据进行完整性保护。 | 符合 | 无 |
| 重要数据存储完整性 | 符合 | 无 |
| 重要信息资源安全标记完整性 | 各类物理设备等系统资源的访问控制信息、重要信息资源安全标记、日志记录等，在OS存储过程中结合HMAC或数字签名等密码技术实现完整性保护，防止重要资源数据被恶意篡改。 | 符合 | 无 |
| 不可否认性 | / | 不适用 | 本系统不涉及电子商务、CA认证、网上银行、证券交易、电子合同、电子公文等（可能涉及法律责任认定的应用），目前没有不可否认性保护需求，故无需部署相关密码产品。 |
| 管理制度 | 具备密码应用安全管理制度 | 建立密码应用安全管理制度,包括密码人员管理、密钥管理、建设运行、应急处置、密码软硬件及介质管理等制度。 | 符合 | 无 |
| 密钥管理规则 | 根据密码应用方案建立相应密钥管理规则。 | 符合 | 无 |
| 建立操作规则 | 对管理人员或操作人员执行的日常管理建立操作规则。 | 符合 | 无 |
| 定期修订安全管理制度 | 定期对密码应用安全管理制度和操作规程的合理性和适用性进行论证和审定，对存在不足或需要改进之处进行修订。 | 符合 | 无 |
| 明确管理制度发布流程 | 明确相关密码应用安全管理制度和操作规程的发布流程并进行版本控制。 | 符合 | 无 |
| 制定执行过程记录留存 | 具有密码应用操作规程的相关执行记录并妥善保存。 | 符合 | 无 |
| 人员管理 | 了解并遵守密码相关法律法规和密码管理制度 | 相关人员应了解并遵守密码相关法律法规、密码应用安全管理制度。 | 符合 | 无 |
| 建立密码应用岗位责任制度 | 建立密码应用岗位责任制度，明确各岗位在安全系统中的职责和权限  1）根据密码应用的实际情况，设置密钥管理员、密码安全审计员、密码操作员等关键安全岗位  2）对关键岗位建立多人共管机制  3）密钥管理、密码安全审计、密码操作人员职责互相制约互相监督，其中密码安全审计员岗位不可与密钥管理员、密码操作员兼任  4）相关设备与系统的管理和使用账号不得多人共用 | 符合 | 无 |
| 建立上岗人员培训制度 | 建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能 | 符合 | 无 |
| 定期进行安全岗位人员考核 | 建立上岗人员培训制度，对于涉及密码的操作和管理的人员进行专门培训，确保其具备岗位所需专业技能 | 符合 | 无 |
| 定期进行安全岗位人员考核 | 定期对密码应用安全岗位人员进行考核 | 符合 | 无 |
| 建立关键岗位人员保密制度和调离制度 | 建立关键人员保密制度和调离制度，签订保密合同，承担保密义务 | 符合 | 无 |
| 建设运行 | 制定密码应用方案 | 依据密码相关标准和密码应用需求,制定密码应用方案 | 符合 | 无 |
| 制定密钥安全管理策略 | 根据密码应用方案,确定系统涉及的密钥种类、体系及其生存生命周期 | 符合 | 无 |
| 制定实施方案 | 按照应用方案实施建设 | 符合 | 无 |
| 投入运行前进行密码应用安全性评估 | 投入运行前进行密码应用安全性评估，评估通过后方可正式运行 | 符合 | 无 |
| 定期开展密码应用安全性评估 | 在运行过程中，严格执行既定的密码应用安全管理制度，应定期开展密码应用安全性评估及功放对抗演习，并跟进评估结果进行整改 | 符合 | 无 |
| 应急处置 | 应急策略 | 制定密码应用应急策略，做好应急资源准备，当密码应用安全事件发生时，应立即启动应急处置措施，结合实际情况及时处置 | 符合 | 无 |
| 事件处置 | 事件发生后，及时向信息系统主管部焖进行汇报 | 符合 | 无 |
| 向有关主管部门上报处置情况 | 事件处置完成后，及时向信息系统主管部门及归属的密码管理部门报告事件发生情况及处置情况 | 符合 | 无 |

**6.8 密码应用部署**

本平台通过部署的SSL VPN安全网关、服务器密码机、国密身份认证系统、传输透明加密系统等密码设备均选自《商用密码产品认证目录》，并调用超算集群系统各项能力对信息系统进行国密加固。密码应用部署拓扑如下图所示：

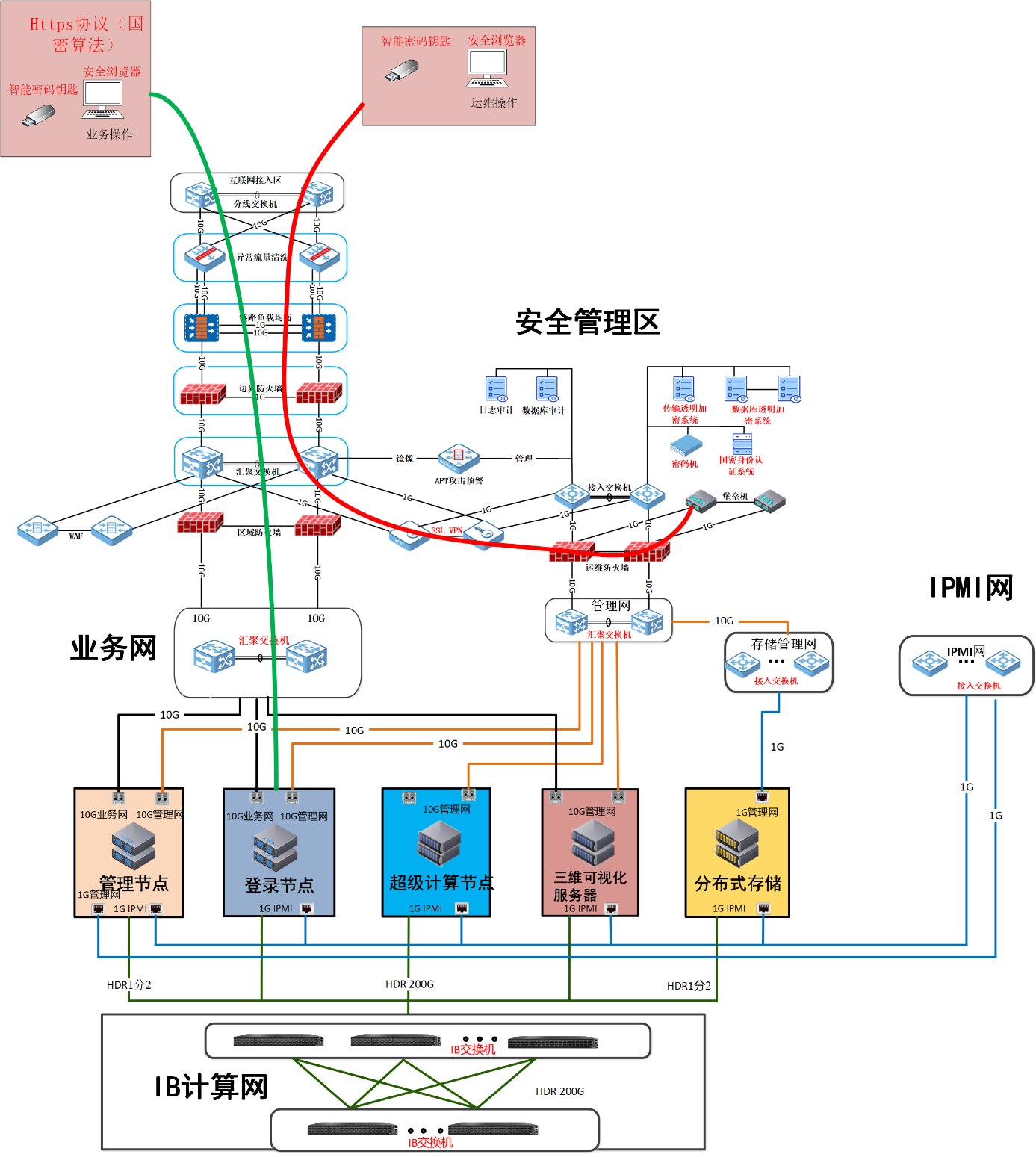


图6-9 密码应用网络拓扑图

**1）SSL VPN安全网关**：主要用于在网络上建立安全的信息传输通道，通过对数据包的加密和数据包目标地址的转换实现远程访问，进行加密通信。

**2）服务器密码机**：实现数据加密、数字签名、随机数生成等功能，保证数据的机密性、完整性。

**3）传输透明加密系统：**系统采用标准国密SM4分组对称加密算法、SM2椭圆曲线公钥密码算法和SM3密码杂凑算法。可为多种操作系统的浏览器终端提供身份认证、加密通信、完整性保护服务。

**4）国密身份认证系统：**基于密钥分割技术和协同签名技术，实现密钥分量在用户终端和服务端独立生成和独立存储。采用国密算法，为浏览器终端提供身份认证服务。

**5）智能密码钥匙**：具备数字证书，采用国密SM2算法实现身份鉴别。

**6.9 密码软硬件产品清单**

表6-1 密码软硬件产品清单

| 序号 | 能力底座 | 使用的密码算法 | 数量 | 用途 |
| --- | --- | --- | --- | --- |
| 1 | SSL VPN安全网关 | SM2/3/4 | 2 | 建立安全的远程管理通道 |
| 2 | 服务器密码机 | SM2/3/4 | 2 | 实现访问控制信息完整性、重要数据存储机密性、完整性保护 |
| 3 | 国密身份认证系统 | SM2/3/4 | 1 | B/S架构应用用户身份鉴别 |
| 4 | 智能密码钥匙 | SM2/3/4 | 500 | 具备数字证书，提供身份鉴别能力 |
| 5 | 传输透明加密系统 | SM2/3/4 | 1 | 互联网场景：PC端浏览器到应用服务端之间数据传输机密性、完整性保护 |
| 6 | 数字证书 | SM2/3/4 | 50 | 提供身份鉴别载体 |
| 7 | SSL站点证书 | / | 1 | 实现网络层面的通信信道身份鉴别、通信数据机密性和完整性 |

**7 安全管理方案**

**7.1 密码应用安全管理制度**

**7.1.1 总则**

1. 为进一步规范XX宁数智能计算产业发展有限公司密码应用信息系统安全管理制度的管理工作，根据《中华人民共和国密码法》、《信息安全等级保护商用密码管理办法》、《商用密码管理条例》、《中华人民共和国网络安全法》和其他有关法律法规的规定，结合本单位实际，特制定本制度。

**7.1.2 制定和发布**

1. 由信息安全负责人组织、指导管理制度的制定、发布与实施；由密码管理部门协同信息安全职能部门，负责管理制度的草拟、论证等工作并上报信息安全主管领导审定。
2. 管理制度应经过由上级机关的信息安全管理部门、公安机关的信息安全等级保护管理部门、信息安全专家组成的论证小组论证通过。
3. 管理制度论证通过后，按照单位公文审核、审批程序，经过领导小组的审定，经信息安全领导小组组长签发后，以单位办文号发布并留存相应发布文件。安全管理制度应注明发布范围，并对收发文进行登记。
4. 安全管理制度应采用统一的公文格式，通过文件形式下发，并进行版本控制在首页右上角标注版本号。[版本号](http://baike.baidu.com/view/421712.htm)由3部分构成，即主版本号+次版本号+修改日期；主[版本号](http://baike.baidu.com/view/421712.htm)第一版为1，只有在重大内容发生变化或内容变动量很大后才发生变化；次版本号第一版为0，每次修订均增加1；修改日期8位，采用施行时的日期；当文档进行任何修改后即编制新的[版本号](http://baike.baidu.com/view/421712.htm)以进行版本控制，例如：1.0.20130701。各文档的版本号独立编制，以最新发布的版本为准。

**7.1.3 评审和修订**

1. 信息安全负责人应组织相关人员对密码应用安全策略体系文件进行评审，并确定其有效执行期限。同时应指定信息安全职能部门每年审视密码应用安全策略系列文件，定期对密码安全管理制度的合理性及适用性进行论证和审定，并保留相关评审记录。当出现以下情况时，可随时组织评审。
2. 密码应用安全法律、法规发生变化；
3. 密码算法和密码技术发生重大变化；
4. 密码应用安全相关的组织机构发生重大变化；
5. 管理机构的管理职责发生重大变化时；
6. 深入剖析审定或论证记录找出存在的不足或需要改进的点形成审定报告，将其作为安全管理制度修订的依据；修订工作应在一个月内完成，并留存相关修订记录。

**7.1.4 附则**

1. 本制度由信息安全相关负责人负责解释。
2. 因违反本制度，发生密码应用安全事件的，按照事件造成的损失和后果，依据国家有关法律法规进行处罚。
3. 本制度自发布之日起执行。

**7.1.5 附件**

**附件1：安全管理文档修订记录**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **修订章节** | **修订内容概要** | **修订日期** | **批准人** |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

注：修订类型包括新增、修改、删除等。

**附件2：安全管理制度评审记录表**

|  |  |  |  |
| --- | --- | --- | --- |
| **评审制度名称** |  | | |
| **评审人员** |  | | |
| **评审日期** |  | **评审地点** |  |
| **评审内容提要：**   1. 评审制度情况； 新增□ 废止□ 修订□ 2. 制度合理性； 是□ 否□ 3. 制度有效性； 是□ 否□ 4. 制度适用性； 是□ 否□ | | | |
| **评审意见：**  **评审人（签字）：**  **年 月 日** | | | |

**附件3：安全管理制度体系评审记录表**

|  |  |  |  |
| --- | --- | --- | --- |
| **评审组人员** |  | | |
| **评审日期** |  | **评审地点** |  |
| **评审内容提要：**   1. 信息安全总体方针、目标的合理性、有效性、充分性； 是□否□ 2. 安全管理制度体系的合理性、有效性、充分性；是□ 否□ 3. 安全管理制度体系文件是否需要修订； 是□ 否□ 4. 体系文件运行现状的评价、缺陷和改进；是□ 否□ 5. 纠正和预防措施，安全检查工作和整改工作是否落实；是□ 否□ 6. 安全管理制度体系需要调整、更新的方针、目标、管理制度、操作规程等内容；   是□ 否□ | | | |
| **评审意见：**  **评审主持人（签字）：**  **年 月 日** | | | |

**7.2 密码应用安全操作规程**

**7.2.1 总则**

1. 为进一步规范XX人工智能超算中心密码应用信息系统管理人员的日常管理操作，根据《商用密码管理条例》和其他有关法律法规的规定，结合本单位实际，制定本操作规程。
2. 本操作规程适用于相关密码应用的人员。

**7.2.2** **密码应用相关人员操作规程**

1. 密钥管理和使用必须指定专人负责，密钥管理员必须是本单位编制的正式员工，密码操作人员与密钥保密管理员分人负责。
2. 密钥管理员需要定期参加岗位培训，具有高度责任感，充分认识到涉密工作的重要性与关键性。
3. 密码设备操作人员要熟悉设备的使用，了解设备在网络中的作用。
4. 密钥存档，由密钥保密管里员统一保密保存。密钥和密码设备必须异地存放。
5. 密码操作人员每次对设备的操作均需要登记记录，并填写《XXXX登记本》。每次向密钥保密管理员借用密钥需要登记记录，并填写《XXXX登记本》，使用后应立即归还，并登记注销。
6. 密码操作人员要定期更换保密设备的密码，并做好登记备案。
7. 制定全面的应急处理预案，在发生密码应用事故时可以及时处理，提高应急事件的处理能力。
8. 密码工作管理员需要定期检查设备的工作状态，保证设备正常工作。
9. 密码安全审计员主要负责对密钥管理员、密码保密管理员的操作行为进行审计分析和监督检查，以及时发现违规行为。
10. 信息系统到涉及的密码设备操作规程详见附件。

**7.2.3** **附则**

1. 本制度由XX人工智能超算中心信息安全相关负责人负责解释。
2. 因违反本制度，发生密码应用安全事件的，按照事件造成的损失和后果，依据国家有关法律法规进行处罚。
3. 本制度自发布之日。

**XXXX设备操作登记表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| XXXX设备操作登记表 | | | | | | | |
| 设备名称 | 操作时间 | 操作事由 | 批准人员 | 操作人员 | 密钥管理员 | 归还时间 | 备注 |
|  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |

**7.3 密码软硬件及介质管理制度**

**7.3.1** **总则**

1. 为了规范XX人工智能超算中心密码软硬件及介质的管理，明确相关人员的职责和权限，保障信息资产管理相关措施的贯彻实施，特制定本制度。

**7.3.2 密码产品安全及管理**

1. 基本规定：

（1）密码软硬件用于保护密钥、产生密钥、PIN的加、解密以及报文鉴别等。这些操作在密码产品中完成，单个完整的密钥和PIN明文不能出现在密码产品之外。

（2）密码软硬件通过国家密码管理委员会办公室审核。

（3）密码软硬件满足中国人民银行颁布的《银行卡联网联合技术规范》、《银行卡联网联合安全规范》以及中国银联颁布的有关规范中规定的基本功能和性能要求。

1. 设备存放及监控：

（1）对关键加密软硬件部署需进行负载均衡，为避免单机故障造成交易失败和密钥丢失；

（2）密码硬件放置在有严格管理的机房内；

（3）密码硬件存放在带锁机柜中，机柜背板固定安装；

（4）对于密码软硬件的操作，配备摄像监控进行全过程监控。

1. 设备操作：

（1）每次对密码软硬件的操作，需经批准后严格按照操作手册、操作规程进行，并记录操作日志；

（2）在应用系统中禁止和密码软硬件非法连接或用做其他用途；

（3）严禁打开密码硬件机壳。

1. 设备启用及报废：

（1）在密码硬件启用之前，确定机壳未被拆卸；

（2）新购买的密码软硬件修改密码软硬件相关缺省口令；

（3）使用IC卡保存密码产品的密钥，在得到IC卡的第一时间更改卡片的缺省密码；卡片分级分人保存；

（4）在密码软硬件报废时，删除存贮在该设备中的密钥。

1. 设备维修与升级：

（1）在密码软硬件报废时，删除存贮在该设备中的密钥；

（2）根据需求提出书面申请；

（3）密码软硬件生产厂商、维护商专人持有效身份证明或介绍信，经证实获准；

（4）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。

**7.3.3 终端设备安全管理**

1. 终端设备操作与监控：

（1）终端设备技术维护人员与日常业务管理人员实行分离，且职责明确；

（2）指定专人管理终端设备；

（3）每次对终端设备的操作，严格按照操作手册、操作规程进行。

1. 设备启用、使用及报废：

（1）在终端设备初始化或更新配置之前，确定如下内容：

①机壳未被拆卸、PIN PAD粘贴封条、密码模块未被非授权修改或替换；

②主密钥生成、装载过程应符合产品操作手册要求；

③主管密码、操作员密码是否为缺省值。

（2）在终端设备报废时，必须立即将存储在该设备中的终端主密钥、工作密钥删除和销毁（包括终端及主机数据库），清除操作员、主管密码，销毁终端软件，并由专人监督检查。

**7.3.4 设备的物理安全**

1. 密码软硬件、终端设备的管理或维护人员定期对设备进行安全检查，主要包括：
2. 设备的物理环境如电源电流及电压、温湿度是否变化；
3. 照明、消防及监控设施是否完好，摄像头是否清晰有效，摄像头不能对准键盘或屏幕；
4. 设备的外壳是否完好，是否有被拆卸、破坏的迹象；
5. 设备有无多余的连接线或外接电缆；
6. 终端设备（如ATM）周围是否张贴有关操作提示；
7. 其他各项安全检查指标是否符合要求。

**7.3.5 介质管理**

1. XX人工智能超算中心信息中心负责存储介质的统一分配及收回。第三方带入介质，如果需要进行数据导入导出时，应向信息中心申请并获得授权，在使用前进行介质杀毒。
2. 介质应储放在安全的环境中,需要做到防磁、防火、防潮，防止损坏；对脱机存放的各类介质（包括信息资源产和软件资产的介质）由专人负责进行检查、控制和保护，以防止被盗、被毁、被修改以及信息的非法泄露
3. 需要携带介质外出时，必须经负责审批。对送出维修或销毁的介质应清除介质中的敏感数据，对关键数据或重要信息的存储介质未经批准不能进行销毁。
4. 相关人员调离时，应将所有信息转交到相关部门，并将必要信息备份到其他介质，并将它从设备中安全的删除，去除原有的口令及其他个人信息
5. 介质应按照信息分类原则进行分类管理，做好信息标识，并且由专人保管。对于重要用途介质不能进行二次信息交换，对重要介质中的数据和软件采取加密存储。

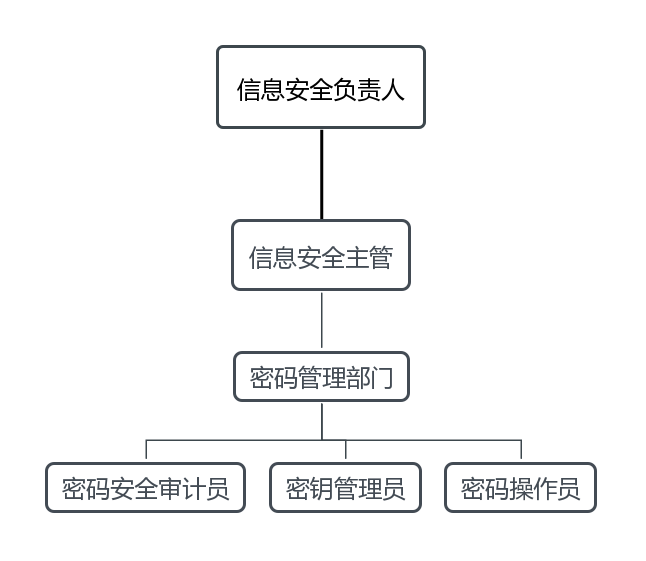
**7.4 密码应用安全组织机构管理制度**

**7.4.1 总则**

1. 为完善XX人工智能超算中心密码应用系统信息安全组织架构，规范和加强XX人工智能超算中心内外网的主机操作系统、网络设备、网络应用系统密码安全应用管理，为数据的保护和加密建立相应的策略，保障XX人工智能超算系统功能的正常运行，特制定本制度。
2. 本管理办法适用于XX人工智能超算中心管理的所有信息应用系统及附属设备；适用于需要账号和密码进行业务操作的相关部门和人员；适用于因业务关系需要使用本单位信息系统的第三方服务商或者供应商。

**7.4.2 组织架构**

1. 由单位主管密码应用信息化工作和保密工作的领导牵头，组织与信息安全相关的各部门负责人，成立密码应用安全组织机构，统筹管理密码应用安全相关工作。
2. XX人工智能超算中心密码应用安全组织机构架构图如下所示：



**7.4.3 岗位职责**

1. 信息安全负责人由信息安全负责人A担任，其岗位职责如下：
2. 领导XX人工智能超算中心的网络安全和信息化工作。
3. 组织落实相关部门下达的网络安全和密码应用信息化工作方针、政策和重大部署。
4. 组织研究、审定XX人工智能超算中心网络与密码应用安全的发展战略、总体规划、重大政策、管理规范和技术标准。
5. 对安全管理的重大更改事项（例如：组织机构调整、关键人事变动、信息系统更改等）进行决策。
6. 组织编制XX人工智能超算中心网络与密码应用安全重大突发事件应急预案，并督促落实。
7. 信息安全主管由信息安全主管B担任，其岗位职责如下：
8. 负责信息安全各类策略的制定、并监督执行，同时根据发展状况持续改进密码应用安全策略。
9. 负责协调各个部门之间的信息安全管理工作，支持和推动密码应用安全工作的实施。
10. 负责信息系统安全状态的监控，监督日常信息安全操作行为；定期查阅信息安全风险评估和检查报告，并监督相关措施的执行情况。
11. 为信息安全应急计划提供资源保障。当信息资产受到严重威胁时，指导并监控应急计划的实施，定期召集相关人员进行应急预案的演练。
12. 密码安全审计员由密码安全审计员1和密码安全审计员2两人担任，其岗位职责如下：
13. 负责对密钥管理员、密码操作员的操作行为进行审计、跟踪分析和监督检查，及时发现违规行为，主要包括系日志分析、安全事件的分析和取证。
14. 对密钥生命周期包括生成、分发与传输、注入与启用、保管、删除与销毁、泄漏与重置各环节全方位、全过程的规范操作与安全管理操作等进行审核和监督操作。
15. 负责密码应用安全审计系统的日常维护，对审计日志进行定期分析和事件记录；发现密钥管理员、密码操作员违规行为或是审计日志中的可疑问题，要及时将审计事件上报信息安全主管领导。
16. 负责相关审计资料的记录、整理、归档等管理工作，配合密码管理部门和技术支持单位进行资料调阅；定期向信息安全主管领导和密码应用系统安全保密管理机构进行审计报告。
17. 负责密码应用安全审查、密码应用安全风险评估、密码应用安全防护监控等工作。
18. 负责与密码应用安全审计有关的其他工作。
19. 密码管理部门由本单位部门领导主导，由涉及密钥生命周期全过程的相关部门共同参加，其岗位职责如下：
20. 按照规定，结合公司的实际状况，制定严格而有效的实施细则，落实岗位责任制。
21. 制订其他有关的安全专项管理制度，对涉及到密钥的生成、传输、保管各个环节的设备提出相应的安全管理要求，如出入登记制度、机房管理制度、岗位操作制度、密钥存储介质管理制度等。
22. 负责密钥生命周期，包括生成、分发与传输、注入与启用、保管、删除与销毁、泄漏与重置等各环节全方位、全过程的规范操作与安全管理。
23. 根据密钥特性，妥善保管密钥组件、密码函、IC密码卡、软件、源代码、涉及密钥安全管理的各种文档。
24. 定期检查密钥安全管理状况，按规定填报有关表格、报告。
25. 密钥管理员由密钥管理员担任。密钥管理员兼任密钥监督员、设备管理员、密钥生成员（注入、接收工作）、档案管理员、密钥销毁员等，以实现密钥全流程安全管理。
26. 密钥监督员岗位职责：

① 负责监督本单位密钥安全管理的各项工作，即在整个密钥生命期内监督生成、保管、注入、分发及销毁等操作的正确性；

② 严格考察本单位重要岗位的工作状况，对不适合密钥维护工作或发现有不良行为的人员，提出调整要求；

③ 制止不正确操作，杜绝违规操作或超越权限操作的行为；

④ 协助完成定期或不定期的专项辅导检查工作。

1. 设备管理员岗位职责：

① 按照本办法有关设备管理的各项规定，维护密码产品等机密设备保持良好的运行状态，凡手续不完备的需求，密码产品管理员有权拒绝；

② 负责对其他密钥维护人员讲解有关生成、装载等操作原理、操作步骤、操作要点和注意事项，指导密钥维护人员将密钥建置在各个相关设备的安全模组内，并在审批表格上记录相关操作情况；

③ 协助完成定期或不定期的专项辅导检查工作。

1. 密钥生成（保管）员岗位职责：

密钥生成（保管）员同时履行注入、保管等岗位职责。

① 按照信息择分、随机性、不可测等原则生成密钥组件；

② 分别保管主密钥组件，键入和改变密钥资料；

③ 接收密钥资料（组件），验证接收到的新密钥资料是否受损；

④ 在监督下销毁密钥组件备份介质；

⑤ 协助完成定期或不定期的专项辅导检查工作。

1. 档案管理员岗位职责：

① 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；

② 维护经管理人员授权后使用密钥的记录，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；

③ 协助完成定期或不定期的专项辅导检查工作。

1. 密钥销毁员岗位职责：

在监督下，完成密钥组件备份介质、文档等密钥资料的销毁。

1. 密码操作员由密码操作员1和密码操作员2两人共同担任，其岗位职责如下：
2. 对密钥系统进行日常操作维护；进行密码系统维护工作；对新用户或新系统进行密码部署工作。
3. 负责加密设备的界面操作，协助完成生成、装载等操作过程。
4. 审查有关审批表格的要求是否合理，操作结束在审批表签名认可；凡手续不完备的申请，操作员有权拒绝。
5. 协助完成定期或不定期的专项辅导检查工作。

**7.5 密码应用安全人员管理制度**

**7.5.1 总则**

1. 为规范XX人工智能超算中心密码应用安全人员管理培训工作，提高人员密码应用安全意识，承担并切实履行各岗位相应的密码应用安全职责，根据《信息安全等级保护商用密码管理办法》、《商用密码管理条例》和其他有关法律法规的规定，结合本单位实际，特制定本制度。
2. 本制度适用于XX人工智能超算中心人员密码应用安全管理的相关活动，包括岗位配置原则、人员录用及调离、

**7.5.2 岗位配置原则**

1. 根据密码应用安全职能要求，结合信息部门实际情况进行人员配备，权限、职能不同的角色必须分离，避免岗位职责存在交叉导致权责不清、责任不明确的现象发生。
2. 为确保密码应用安全工作的顺利开展，保障信息系统的正常运行，须结合单位实际情况设置密钥管理员、安全审计员、密码操作员等关键岗位并明确其岗位职责。
3. 根据相关密码管理政策、数据安全保密政策规定，对密钥管理员、安全审计员、密码操作员等关键岗位配备多人，以实现多人共管机制，达到互相制约、互相监督的目的，其中安全审计员岗位不可与密钥管理员、密码操作员兼任，保障信息系统的良好运行。
4. 相关设备及系统的管理和使用账号应配置专人管理，仅限本人使用不得外借他人使用，避免账号多人共用现象的发生，对信息系统安全造成威胁。

**7.5.3 人员录用及调离**

1. 信息安全负责人负责指导人事部门对密码应用安全工作人员的录用工作。应对拟录用人员进行身份、背景、专业资格和资质等方面的审查，并进行相应技能考核，并留存相关审查文档或记录，合格者需签署保密协议方可上岗。密钥管理员、密码操作员应从本单位在编的正式员工中选拔。
2. 人员调离时必须终止其所有的访问权限，涉及相关信息系统账号、口令时，先采取更换密码或冻结账号的措施，避免直接删除账号；并列出信息资产交接清单，清单内容应包括其使用的账号名、密码、权限、各种身份证件、钥匙等以及其他相关信息资料、资产和软硬件设备，信息安全管理部门和归还资产接收部门进行审核和确认。
3. 密码应用安全人员内部调动至其他岗位时，在接到岗位调动通知后，应于规定的日期内依据调动程序办理好工作及资料的移交手续后才能前往新岗报到。管理层和密钥管理员、安全审计员、密码操作员等关键岗位人员调离岗位，必须签署书面保密承诺书，承诺在调离岗后根据保密承诺书的内容履行相关的保密责任和义务；涉密人员实行脱密期管理制度，进行离岗安全审查，在规定的脱密期限后，方可调离；经人事部门严格按照人事管理规定办理调离手续，留存调离手续的相关记录。

**7.5.4 培训与考核**

1. 为保证人员能够充分履行密码应用安全职责，应每半年组织一次针对密码应用安全相关人员的密码应用安全教育和培训，使得密码应用安全相关人员对商用密码相关法律法规有一定了解并遵守，通过培训具备正确使用商用密码产品的能力；培训内容包括密码相关法律法规学习、安全意识的培养、密码产品的使用方法以及密码安全技术培训等，相关培训负责人对培训内容进行记录和留存。
2. 根据各个岗位的业务应用、安全意识和保密意识需求制定考核计划，定期对各岗位人员进行安全理论知识和安全技能水平的考察，针对考核内容制定相应奖惩机制，并纳入到年底绩效考核奖励中，相关负责人将考核内容及结果进行记录和保存。

**7.5.5 附件**

《XXXXXX员工保密协议》

**附件1：《人员保密承诺协议书》**

甲方（人员）：

乙方（单位）：（系统责任单位）

鉴于甲方在乙方任职并将获得乙方支付的相应报酬，双方当事人就甲方在任职期间保守乙方交易秘密、经营秘密、管理秘密、技术秘密的有关事项，制定下列条款并共同遵守：

第一条 甲方在乙方任职期间，对甲方职责范围内所接触到的交易秘密、经营秘密、管理秘密、技术秘密和商业秘密负有保密义务。在未征得乙方的同意，不得任意篡改和泄露以上秘密。

第二条 甲方在乙方任职期间，应本着谨慎、诚实的态度，维护其于任职期间知悉或者持 有的虽属于第三方但乙方承诺有保密义务的交易秘密、经营秘密、管理秘密、技 术秘密和商业秘密信息，以保持其机密性。

第三条 甲方承诺未经乙方同意，不得以泄露、告知、公布、发布、转让或者其他任何方式使任何人知悉属于乙方或者虽属于第三方但乙方承诺有保密义务的交易秘密、经营秘密、管理秘密、技术秘密或其他商业秘密信息，也不得在履行职务意外使用这些秘密信息。

第四条 甲方承诺，在为乙方履行职务时，不得擅自使用任何属于侵犯第三方的交易秘密、 经营秘密、管理秘密、技术秘密或其他商业秘密信息，并不得擅自实施可能侵犯 第三方知识产权的行为，若违反上诉承诺而导致乙方遭受第三方的侵犯指控时， 甲方应当承担乙方为应诉而支付的一切费用；乙方因此而承担侵权赔偿责任的，有权向甲方追偿。

第五条 甲方承诺，其在乙方任职期间，非经乙方事先同意，不在与乙方生产、经营同类 产品服务的其他企事业单位、社会团体内担任任何职务。

第六条 甲方因职务上的需要所持有或保管的一切记录着乙方秘密信息的文件、资料、图表、笔记、报告、信件、传真、磁带、光盘、硬件存储设备、仪器以及其他任何形式的载体，均归乙方所有，而无论这些秘密信息有无商业上的价值，若必须随同载体一并上交的，乙方支付给甲方该些载体产品成本费。

第七条 甲方应当于离职时，返还全部属于乙方的财物，包括记载着乙方秘密信息的一切载体。当记录着秘密信息的载体是由甲方自备的，且秘密信息复制到乙方享有所有权的其他载体上并把原载体上的秘密信息消除。

第八条 本协议提及的交易秘密、经营秘密、管理秘密、技术秘密和商业秘密指不为公众所知悉、能为乙方带来经济利益且采取本协议所述保密措施的技术信息，包括：商品信息、经营方针、经营规划和策略、广告策略、决策和市场意向、管理文件、行政文件、经营文件、技术方案、技术规范、计算方法、设计文件、科研成果及技术文档等等。

本协议提及的其他商业秘密指不为公众所知悉、能为乙方带来经济利益且采取本协议所述保密措施的商业信息，包括：客户资料、销售资料、业务资料、财务资料等等。

第九条 双方解除或终止劳动关系后，甲方不得向第三方公开乙方所拥有的未被公众所知悉的各项秘密。

第十条 保密期限：

1. 劳动期内；

2. 乙方的保密内容未被公众知悉期内。

第十一条 脱密期限：

1. 因履行劳动协议约定条件或劳动关系发生变化，甲方要等解除劳动关系的必须以书面形式提前一个月通知甲方，由乙方采取脱密措施，安排甲方脱离涉密岗位，甲方应该接受乙方的工作安排并完整办妥涉密资料的交接工作。

2. 劳动关系终止双方无意续约的，提出方必须以书面形式提前一个月通知对方， 由乙方采取脱密措施，安排甲方脱离涉密岗位；甲方应该接受乙方的工作安 排并完整办妥涉密资料的交接工作。

3. 劳动关系解除或期满终止后，甲方必须信守本协议，不损害乙方的利益。

第十二条 本协议中所称的任职期间，以甲方从乙方领取工资为标志，并以该项工资所代表的工作期间为任职期间。本协议中所称的离职，以任何一方明确表示解除或辞去聘用关系的时间为准。甲方拒绝领取工资且停止履行职务的行为，视为提示辞职。

第十三条 因本协议而引起的纠纷，如果协商解决不成，任何一方均有权提起诉讼。双方同意，选择乙方所住地的、符合级别管辖规定的人民法院作为双方合同纠纷的第一审管辖法院。

第十四条 违约责任

1. 在劳动关系期内，甲方违反此协议，未造成乙方经济损失，但给乙方正常经营活动带来麻烦的，乙方有权调离甲方涉密的岗位，停发红利奖金，并予以行政处罚；

2. 在劳动关系期内，甲方违反此协议，造成乙方经济损失的，乙方可解除甲方的劳动关系，并追索经济损失赔偿，构成犯罪的，上诉人民法院，依法追究 甲方刑事责任。

3. 劳动关系解除或期满终止后，甲方未信守本协议，造成乙方利益损害的，乙方保持追究甲方法律责任的权利，构成犯罪的，交由司法机关处理。

第十五条 本协议自双方签字或盖章完成之日起生效。

第十六条 本协议如与双方以前的口头或书面协议有抵触，以本协议为准。本协议的修改必 须采用双方同意的书面形式。

甲方签字（盖章）： 乙方（盖章）：

身份证号码： 中心负责人：

年 月 日 年 月 日

**附件2：安全岗位考核表**

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 被考评  对象 |  | 部门 |  | 职务 |  | 总得分 |  |
| 考评人 |  | 考评  时间 | 至 | 填表时间 |  |
| 考核项目 | 细分指标 | 权重（分） | 指标具体内容  及定义 | 自我评价  得分 | | 考核评价得分 | |
|
|
| 个人专业知识与技能提升（5分） | 专业知识 | 2 | 运维技术岗位的专业知识（基础知识、业务知识、关联知识）。 |  | |  | |
| 专业技能 | 3 | 运维技术岗位的专业技能。 |  | |  | |
| 综合能力（25分） | 分析判断与应变能力 | 4 | 能对复杂的问题进行正确判断，处理工作事务机敏灵活，并在自己职权范围内能迅速而准确地对多种备选行动方案进行评价，并作出最终决定。 |  | |  | |
| 问题解决能力 | 4 | 根据现场的突发事件，能够从多方面进行分析，找出故障原因，从而解决问题。 |  | |  | |
| 执行能力 | 5 | 对上级的命令、下达的计划、布置的工作能及时贯彻执行，并及时复命。 |  | |  | |
| 创新能力 | 4 | 在处理工作事务时，运用新思维、新方法提高工作效率和效益。 |  | |  | |
| 表达及沟通能力 | 4 | 能清楚、完整地向对方充分说明及表达自己的想法而使其理解，并能聆听及尊重对方的意见。 |  | |  | |
| 协调及人力关系能力 | 4 | 作为组织的一员，能够自觉地与组织内其他成员保持良好合作关系，热情协助他人的工作，积极参加公司及部门内部的各种活动，维护良好的同事关系。 |  | |  | |
| 品质与  态度  （10分） | 道德品质 | 2 | 诚实正直、以身作则、克己奉公、乐于助人。 |  | |  | |
| 责任感 | 2 | 充分理解自己的责任和义务，不回避责任，在期限之内完成上级交付的工作，主动地以主人翁的态度去完成工作。 |  | |  | |
| 纪律性 | 2 | 理解和遵守公司的各项规章制度、服从上级的指示和命令，出勤率高。 |  | |  | |
| 自信心 | 1 | 对工作目标以及自己的决定充满信心。 |  | |  | |
| 工作热情 | 1 | 工作积极主动，经常愿意挑战艰难性工作。 |  | |  | |
| 合作精神 | 2 | 在本部门内和关联部门间与同事相互配合及协作的态度。 |  | |  | |
| 专项考评（60分） | 安全意识 | 15 | 充分理解自己的责任和义务 |  | |  | |
| 密码操作管理技能 | 20 | 实际操作熟练程度 |  | |  | |
| 网络安全法 | 10 | 熟悉《中华人民共和国网络安全法》程度 |  | |  | |
| 密码相关法律法规的考核 | 15 | 熟悉《密码法》程度 |  | |  | |
| 合计 | | | |  | |  | |

**附件3：安全岗位培训记录表**

**安全相关培训记录表**

|  |  |  |  |
| --- | --- | --- | --- |
| 培训时间 |  | | |
| **培训地点** |  | | |
| **参会专家/讲师** |  | | |
| **培训内容** |  | | |
| **参会人员签到** | **人员** | **单位/部门** | **签字** |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

**7.6 密码应用建设运行管理制度**

**7.6.1 规划建设**

1. 信息系统规划阶段，本单位应依据密码相关标准和密码应用需求，制定密码应用方案，并组织专家或测评机构进行评审，将评审意见作为项目规划立项的重要材料，积极落实整改建议，提高密码应用安全性。
2. 根据制定的密码应用方案，确定系统涉及的密钥种类、体系及其生存周期环节，及其各环节密钥要求。
3. 密码应用信息系统中采用的密码协议和技术应遵循密码相关国家及行业标准；系统中应使用通过国家密码管理部门核准，具有商用密码产品型号证书的密码产品与密码模块。
4. 按照国家相关标准，制定实施方案，方案内容应包括但不少于信息系统概述、安全需求分析、商用密码系统设计方案、商用密码产品清单（包括产品资质、功能及性能列表和产品生产单位等）、商用密码系统安全管理与维护策略、商用密码系统实施计划等。

**7.6.2 运行维护**

1. 密码应用信息系统投入运行前，应经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。
2. 对运行关键业务的系统进行监控，监控系统关键性能参数（如启动参数）、工作状态、占用资源和密钥使用情况等内容；对系统运行情况进行记录，每月对记录结果进行分析、统计，并形成分析报告。
3. 密码应用信息系统投入运行后，严格执行XX人工智能超算中心的密码应用安全管理制度。应每年组织密码应用安全性测评机构对系统进行密码应用安全性评估和攻防对抗演习，依据评估报告及整改建议，积极落实整改工作；若系统存在重大安全隐患,应立即停止系统运行并制定整改方案，整改完成后系统方可再次投入运行。

**7.6.3 备份与恢复**

1. 按照备份策略，对不同业务数据采用不同备份方式，灵活运用完全备份、增量备份和差异备份等方式进行备份，保证信息系统出现故障时，能够满足数据恢复的时间点和速度要求。
2. 每次备份必须进行备份记录，对备份介质类型、备份的频率、数据量、数据属性等有明确描述，并及时检查备份的状态和日志，确保备份是成功的。
3. 定期对介质做恢复测试，至少一年两次。

**7.7 密码应用安全应急管理制度**

**7.7.1 总则**

1. 为科学应对密码应用安全突发事件、建立健全信密码应用安全应急响应机制，有效预防、及时控制和最大限度地消除密码应用安全各类突发事件的危害和影响，特制定本应急预案。

**7.7.2 事件分类定级**

1. 安全事件分为有害程序事件、网络攻击事件、信息破坏事件、信息内容安全事件、设备设施故障、灾害性事件和其他信息安全事件等7个基本分类。为保障本预案符合单位面临的，将安全事件依据其性质、危害程度、涉及范围、影响大小等情况，由高到低划分为四个等级，即：特别重大事件（Ⅰ级）、重大事件（II级）、较大事件（III级）和一般事件（IV级）：
2. 特别重大（I级）：指能够导致特别严重影响或破坏的信息安全事件。会使公司特别重要信息系统遭受特别重大的系统损失，即造成系统大面积瘫痪3小时以上，使其丧失业务处理能力，或系统关键数据的保密性、完整性、可用性遭到严重破坏；
3. 重大（II级）：指能够导致严重影响或破坏的信息安全事件。会使公司特别重要信息系统遭受重大的系统损失，造成系统3小时内中断或局部瘫痪，使其业务处理能力受到极大影响，或系统关键数据的保密性、完整性、可用性遭到破坏；
4. 较大（III级）：指能够导致较严重影响或破坏的信息安全事件。会使公司特别重要信息系统遭受较大的系统损失，造成系统中断，明显影响系统效率，使重要信息系统或一般信息系统业务处理能力到影响，或系统重要数据的保密性、完整性、可用性遭到破坏；
5. 一般（IV级）：指能够导致较小影响或破坏的信息安全事件。会使公司特别重要信息系统遭受较小的系统损失，造成系统短暂中断，影响系统效率，使系统业务处理能力受到影响，或系统重要数据的保密性、完整性、可用性遭到影响；

**7.7.3 事件处理程序**

1. 根据安全事件等级制定相应的应急预案及管理制度，明确应急事件处理流程及管理措施，并严格执行且留存相关事件处理记录。
2. 发生重大（II级）或特别重大（Ⅰ级）信息安全事件：
3. 及时上报上级主管部门及同级密码管理部门，并协同相关单位成员尽快组织专家组对突发事件性质、级别及启动预案的时机开展评估，向是上级主管部门提出启动预案的建议，报上级主管部门批准。
4. 在上级主管部门做出启动预案决定后，立即启动应急处理工作。
5. 发生一般（IV级）或较大（III级）信息安全事件：报信息安全主管直接启动应急预案，争取在第一时间内恢复运行。
6. 安全事件处置完成后，转入常态化管理，应急小组应回顾并整理发生事件的各种相关信息，尽可能地把所有情况记录到文档中并存档保管。并将相关事件处置结果及情况上报同级密码管理部门。

**7.8 密钥安全管理规范**

**7.8.1 密钥设备管理规范**

1. XX人工智能超算中心密钥采用通过国密认证的服务器密码机进行管理。密码机采用的防拆、防撬结构设计，利用全密封机壳、物理锁控制开启面板等技术为密钥的管理提供了强有力的保护。采用先进的RAM供电保护电路的实现。内置IP防火墙技术，提供IP包过滤，只有授权的用户才可以访问密码机，使用密码机的安全功能。满足随意开关机的要求，可保证在出现意外掉电或人为随意关机的情况时，不会造成系统损坏。
2. 设备运行规范。密码机只在生产系统内网中工作，系统中主机访问密码机必须通过防火墙；在密码机中禁止为与密码操作无关的主机设备设置访问权限；密码机损毁、报废或不再使用时，执行毁钥操作。

**7.8.2 密钥生命周期的安全管理**

1. 包括密钥的生成、分发、导入、使用、存储、备份、更新、销毁等内容。其任务就是在整个生命周期内严格控制密钥的使用，直到它们被销毁为止，并确保密钥在各个阶段或环节都不会出现任何纰漏。
2. 密钥生成。主密钥、密钥加密密钥、身份认证密钥和业务密钥由专用密钥生成设备随机生成，其中主密钥生成后的明文形式由三段密钥组件构成，分别存储在三处介质中。
3. 密钥分发。密钥在传输时采用双重控制，将密钥分为不同的密钥分量，采用不同传输渠道和不同传输时间，分别分发密钥分量。
4. 密钥导入。密钥分量需分人管理，密钥导入时应分人并在隔离状态下导入密码设备；密钥导入完成后，按规定填写相关的密钥导入记录表格。
5. 密钥存储。主密钥、密钥加密密钥、身份认证密钥、业务密钥均存储在密码机内部。
6. 密钥使用。主密钥、密钥加密密钥、身份认证密钥、业务密钥均在密码机内部使用。
7. 密钥备份。使用硬件密码卡对主密钥的密钥分量和密钥加密密钥、身份认证密钥、业务密钥进行备份，密钥对于密钥和密钥分量的存储，坚持三个原则：最小化、认可化和高安全性。

**最小化**：由指定专人负责保管密钥组件，且不同成分的密钥组件由不同人员保管；

**认可化**：密钥组件存放在封条封装的信封内，只有指定的密钥管理员可以拆分信封；

**高安全性**：封装密钥的信封存放在不同的保险箱内，指定的密钥保管员才有保险箱的密码和钥匙。

对于密钥生成和导入密码设备，设有专人进行配置和维护，密钥保管员无权限开启和操作设备。

1. 密钥更新。除密钥泄漏或可能泄漏外，主密钥一般不更新。密钥加密密钥1-2年更新一次或一般不更新。若出现泄漏，则立即更换被怀疑或确认泄密的密钥，确定被涉及到的功能领域，并且向相关管理部门报告。若主密钥、密钥加密密钥和身份认证密钥出现泄漏，采用与初次生成相同的方式产生新的主密钥、密钥加密密钥和身份认证密钥；若主密钥泄漏，则替换主密钥并替换所有由该主密钥保护的密钥。若密钥加密密钥泄漏，则替换密钥加密密钥并更换使用该密钥加密的所有密钥。业务密钥每次会话都进行更新，若怀疑泄漏，则采用人工方式断开连接，重新分配业务密钥。
2. 密钥销毁。密钥生成后或在系统更新、密钥组件存储方式改变等情况时，不再使用的密钥及密钥组件或相关信息的资料均及时销毁。作废或被损坏的密钥在双人控制下安全销毁，保证无法被恢复，销毁过程由专人监控和记录。

**7.8.3 管理规定与监督检查**

1. 组建密钥安全管理工作组
2. 组织形式：密钥工作组由本单位部门领导任组长，由涉及密钥生命周期全过程的相关部门共同参加。
3. 工作职责：
4. 按照规定，结合XX人工智能超算中心的实际状况，制定严格而有效的实施细则，落实岗位责任制；
5. 制订其他有关的安全专项管理制度，对涉及到密钥的生成、传输、保管各个环节的设备提出相应的安全管理要求，如出入登记制度、机房管理制度、岗位操作制度、密钥存储介质管理制度等。
6. 负责密钥生命周期，包括生成、分发、导入、备份、使用、更新、销毁等各环节全方位、全过程的规范操作与安全管理。
7. 根据密钥特性，妥善保管密钥组件、密码函、IC密码卡等涉及密钥安全管理的各种文档。
8. 定期检查密钥安全管理状况，按规定填报有关表格、报告。
9. 审批制度。对密钥的任何操作必须履行相关审批手续，执行表格登记制度，未经履行审批手续的操作过程一律视同为违章操作，应严格禁止。
10. 应急措施。根据本单位的具体情况制定应急措施以防范以外因素导致的业务无法正常运营，应急措施包括申请审批手续、启动与恢复流程、记录操作日志等内容。
11. 监督。按照严格按要求做好自查，并配合做好相关监督与调查工作。

**7.8.4 附则**

1. 本文件由XX人工智能超算中心信息安全领导小组负责制定、解释、修改和完善。
2. 本文件自发布之日起实行。

**8 实施保障方案**

为保障密码应用项目的顺利推进,特制定以下各项工作措施予以保障。

**8.1 项目组织架构**

从现有的优秀技术人员和管理人员中抽取合适的人选构成建设项目团队，并将通过对整个工程开发实施的具体要求及相关人员的安排，能使参与工程开发实施的人员理解该项目的目标，明确各自的责任，从而降低计划延期和预算超支的风险。

根据本项目各部分工作内容性质，具体分成四个组来承担：项目协调组、安全服务组、产品实施组和文档组，各组安排相应的组长来管理和领导，并对项目经理负责。



**8.2 组织职责说明**

**8.2.1 项目经理**

* 负责本项目的总体成功实施；
* 直接对客户满意度负责；
* 负责领导管理各个小组；
* 负责项目的整体设计，对本项目的整体技术负责；
* 对实施行为和结果的质量、进度负责；
* 向项目建设项目工程项目负责人报告项目实施的进度结果。

**8.2.2 项目协调管理小组（质量负责人、项目技术负责人）**

* 根据项目计划安排执行必要的活动；
* 负责协调客户相关人员；
* 负责安排项目组的后勤工作；
* 接受项目经理的领导。

**8.2.3 安全服务组（技术人员）**

* 负责本项目的安全服务工工作的落实，包括制定详细实施方案；
* 负责本项目安全服务的实施、用户培训等实施工作；
* 对责任范围内的质量、进度及技术负责；
* 直接对客户满意度负责；
* 接受项目经理的领导。

**8.2.4 产品实施小组（售后工程师）**

* 负责本项目产品的用户环境的调研收集、制定详细实施方案及系统测试方案；
* 负责本项目各个产品设备的安装、配置、调试、试运行、用户培训等实施工作；
* 对责任范围内的质量、进度及技术负责；
* 直接对客户满意度负责；
* 接受项目经理的领导。

**8.2.5 文档小组**

* 负责制定和执行本项目有关规范和标准；
* 负责制定和执行本项目系统实施的质量保证计划；
* 负责本项目的相关文档工作；
* 对责任范围内的质量、进度及技术负责；
* 接受项目经理的领导。

**8.3 检查监督管理**

项目实施质量保证工作涉及项目各阶段的活动，应该特别注意项目的早期评审工作，以确保在项目实施的各个阶段和各个方面都认真采取各项措施来保证与提高实施的质量。在建设过程中我方建议应进行如下几类评审与检查工作：

**阶段评审：**在系统实施过程中，需要定期地或阶段性地对系统和文档进行评审。我方建议在本项目中应至少进行以下三次评审：第一次评审方案合理性、确认验收方法；第二次评审方案的实施计划，实施步骤、测试方法，试运行方案等，并对第一次评审结果复核；第三次评审功能和综合检查。阶段评审要组织专门的评审小组，评审小组原则上由实施小组成员、用户项目管理小组成员、承建方代表等构成。

**日常检查：**在本项目实施过程中，各子系统应该填写项目进展报告，即各个设备调试进展报告、软件安装部署阶段进度表、项目完成情况表等三张表格。项目管理人员可以通过项目进展报告发现有关项目实施过程中的问题。

**项目验收：**我方建议组织专门的验收小组对项目成果进行验收，各小组协助其工作。验收工作应该按照双方都认可的验收规程正式履行验收手续。验收内容应包括文档验收、设备验收、功能测试等几项工作。具体的验收规程另行制订。

**8.4 项目质量保障**

通过规范、明确和落实技术开发人员的质量控制职责，在本项目执行过程中实施全面的质量管理计划，从系统方案分析、设计、实施、测试等阶段环节，设立质量控制点，落实质量管理任务，规定各种必要的质量保证措施，以保证所交付的系统能够符合项目合同书规定的各项规定，满足用户的各项需求。

文档是项目管理的重要组成部分，是项目实施周期各个不同阶段的产品描述。承建方的质保体系主要从完备性、正确性、简明性、可追踪性、自说明性和规范性等六个方面对文档进行评审，验证和确认各阶段文档的合适性。

在项目实施过程中向客户提交的文档主要有：

* 密码应用方案
* 项目实施方案
* 设备安装确认书
* 用户测试确认报告（STR）
* 用户手册（SUM）
* 项目进展报表（PPR）
* 阶段评审报表（PRR）
* 项目实施总结（PDS）
* 应急处置方案