**5 密码应用技术方案**

本方案根据最终版测试系统密码应用改造要求和相关建设的整体规划，以及密码应用的合规性、正确性和有效性，保证密码应用改造的正确实施部署，来采用此套密码应用技术方案。

## 5.1 密码应用技术框架（陈凯）

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

密码应用技术总体架构如图 5.1所示。



图 5.1 密码应用技术架构

其中：

{{\*51list }}

## 5.2 物理和环境安全（董涵宁）

物理和环境安全要求，采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，保护物理访问控制身份鉴别信息。符合该标准的电子门禁系统使用SM4等算法进行密钥分散，实现门禁卡的一卡一密，并基于SM4等算法鉴别人员身份。

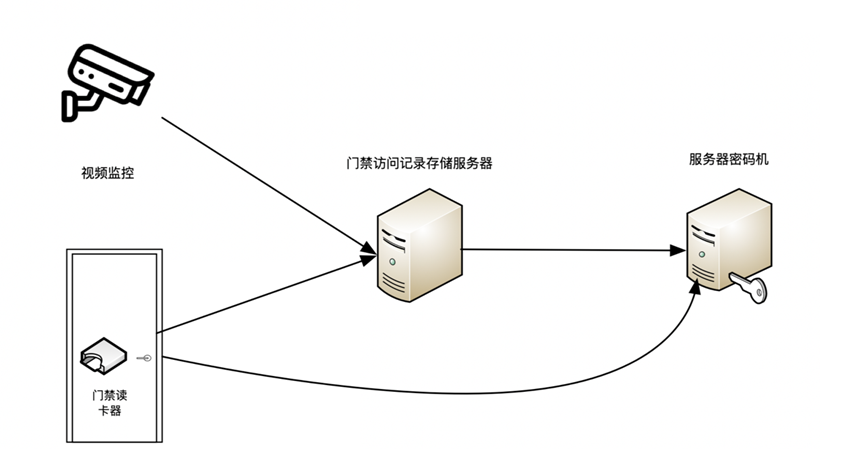


图 5.4 物理环境图

1. 身份鉴别：由于是租用机房，存在无法对机房进行改造的问题。但考虑到机房未使用遵循GM/T 0036要求的国密电子门禁系统，不满足物理和环境安全中的高风险项身份鉴别的有关要求。物理和环境安全中的身份鉴别属于高风险项，指标要求采用密码技术进行物理访问身份鉴别，保证重要区域进入人员身份的真实性。但考虑到系统门禁系统现状和资金问题，也可使用缓解措施，请检查目前机房措施是否满足此高风险项的缓解措施：采用基于生物识别技术（如指纹等）对进入人员进行身份鉴别；如指纹、人脸识别的门禁系统；采用基于普通电子门禁系统并配合人工登记和视频监控，保证重要区域进入人员身份的真实性。采用如上两种方式，属于此高风险项的缓解措施，可酌情降低风险等级。若不满足如上要求，存在无法通过此高风险项的风险。
2. 电子门禁记录数据存储完整性：采用基于密码技术的遵循GM/T 0036要求的电子门禁系统，电子门禁系统进出记录应严格进行完整性保护，完整的进出记录是实现安全管理、事后追责的重要基础。符合该标准的电子门禁系统使用采用MAC或数字签名等技术对记录进行完整性保护，保证进出数据记录的存储完整性。
3. 视频监控记录数据存储完整性：采用基于密码技术的的视频监控系统，视频监控系统的音像记录应严格进行完整性保护，完整的音像记录是实现安全管理、事后追责的重要基础。使用采用MAC或数字签名等技术对记录进行完整性保护，保证视频监控音像记录数据的存储完整性。

表 5.1 物理和环境安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 物理和环境安全 | 机房1 |
| 2 | 物理和环境安全 | 机房2 |

## 5.3 网络和通信安全（贾红豆、陈凯、曹冉筝）

网络与接入安全密码应用，在应用系统接入边界部署安全网关，配合远程终端在应用系统，对访问应用业务系统的用户进行身份鉴别和权限控制，对传输的数据进行机密性和完整性保护。

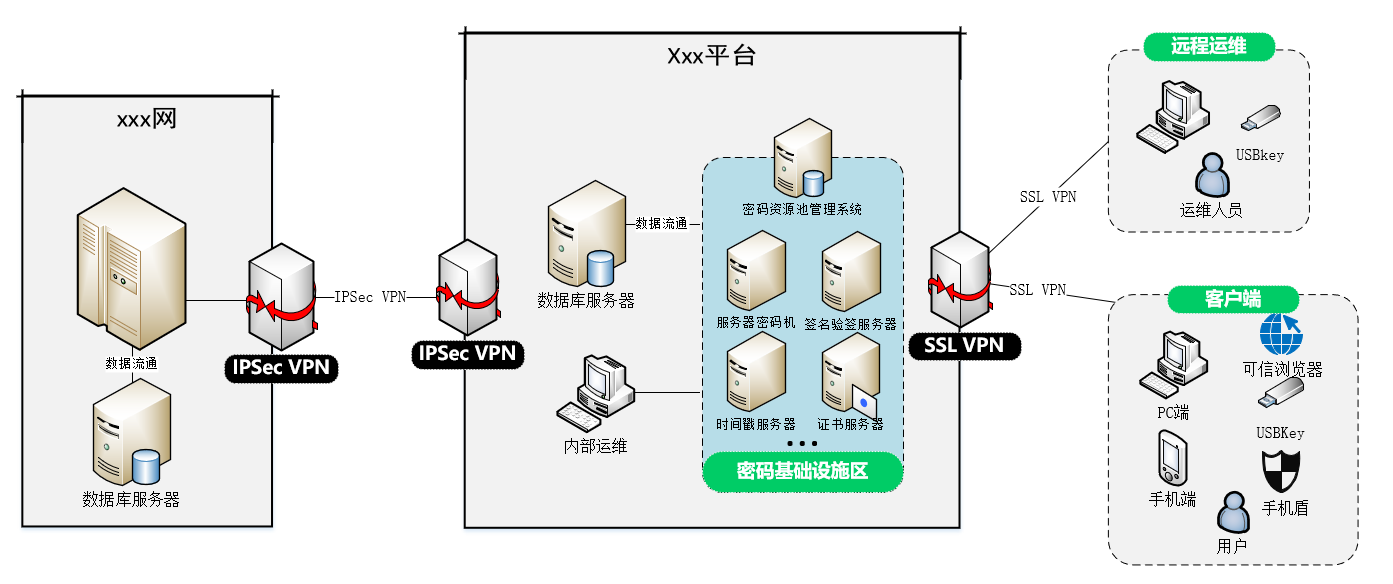


图 5.5 网络和通信安全架构图

1、互联网VPN客户端与内网SSL VPN之间的通信信道

1. 身份鉴别：在机房网络边界处部署SSL VPN安全网关，并将TLS协议配置成采用核准的密码套件，需通过SSL VPN网关连接到业务系统，并向用户配发USBKey，实现对用户的安全身份鉴别，防止与假冒实体通信。
2. 通信数据完整性：部署的SSL VPN安全网关已通过商用密码机构认证，利用SSL VPN本身的机制保证通信数据完整性。
3. 通信过程中重要数据的机密性：部署的SSL VPN安全网关已通过商用密码机构认证，利用SSL VPN本身的机制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：部署的SSL VPN安全网关已通过商用密码机构认证，利用SSL VPN本身的机制保证网络边界访问控制信息的完整性。
5. 安全接入认证：部署的SSL VPN安全网关已通过商用密码机构认证，通过建立SSL安全传输通道，支持在标准的SSL协议下，通过数字证书实现加密传输，来确保用户接入安全。

表 5.2 网络与通信安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 网络和通信安全 | 通道1 |
| 2 | 通道2 |

## 5.4 设备和计算安全（卢焱、王晨、曹冉筝）

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



图 5.6 设备和计算安全架构图

1. 身份鉴别：本系统已使用国密安全堡垒机实现身份鉴别。本系统由经批准的证书认证系统提供数字证书，在密码基础设施区部署堡垒机和签名验签服务器。运维人员配发USBKey（USBKey中存有数字证书），运维人员在PC端使用用户名+口令+USBKey的方式保证身份的真实性；登录堡垒机时验证运维人员的签名证书，通过后选择对应的应用服务器、数据库服务器等设备，通过SSH协议对系统中的各业务应用服务器、各数据库服务器进行运维管理。以此实现对运维人员的安全身份鉴别，防止非授权人员登录。
2. 远程管理通道安全：运维人员先登录到堡垒机，由堡垒机对设备进行集中管理，运维人员选择对应的设备登录，进行运维操作。
3. 系统资源访问控制信息完整性：对本系统涉及到的：（1）Windows系统访问控制信息；（2）系统文件目录的访问控制信息； （3）SQL Server数据库中的数据访问控制信息；在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护。（所涉及的Windows系统权限访问控制信息一般存储在本地计算机SAM文件中，路径一般为C:\Windows\System32\config，具体存储文件和路径需参考目标系统操作系统及其版本号；所涉及的SQL Server数据库中的数据访问控制信息，具体存储文件和路径需参考目标系统数据库及其版本号）
4. 重要信息资源安全标记完整性：本系统不涉及重要信息的敏感标记。
5. 日志记录完整性：本系统已调用合规密码服务，对应用服务器、数据库服务器等设备日志记录进行完整性保护。
6. 重要可执行程序完整性、重要可执行程序来源真实性：在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性。

表 5.3 设备与计算安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 设备和计算安全 | 设备1 |
| 2 | 设备2 |

## 5.5 应用和数据安全（冯天浩、张海政、刘双平）

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



图 5.7 应用和数据安全架构图

1. 身份鉴别：管理员通过PC端登录业务系统时，使用账号+密码配合智能密码钥匙登录系统，智能密码钥匙采用冲击-响应方式认证，并在密码基础设施区部署服务器密码机，提供验证运算。系统管理员通过可信浏览器将智能密码钥匙中的证书发送到签名验签服务器，签名验签服务器对证书进行校验，并结合国密SSL登录。
2. 系统应用访问控制信息完整性：在密码基础设施区部署服务器密码机，使用HMAC算法对系统应用的用户角色分配表、系统权限分配表、数据库权限分配表等访问控制信息进行完整性保护，防止访问控制信息被篡改。
3. 重要信息资源安全标记完整性：无（系统中不存在重要信息安全标记）
4. 重要数据传输机密性：客户端与服务端进行通信时，除在网络和通信层面搭建SSL安全通信链路对重要数据传输进行机密性保护外还需要在应用层实现重要数据传输的机密性保护：应用系统通过国密安全密码应用中间件数据加解密接口调用服务器密码机，采用SM2算法进行会话密钥交互，使用会话密钥采用SM4算法加密。服务端与服务端进行通信时，除在网络和通信层面搭建IPSec安全通信链路对重要数据传输进行机密性保护外还需要在应用层实现重要数据传输的机密性保护：应用系统通过国密安全密码应用中间件数据加解密接口调用服务器密码机，采用基于ECC密码算法的数字信封功能，先使用对称密钥加密数据，再使用接收方公钥对对称密钥加密。
5. 重要数据存储机密性：在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用SM4算法对数据信息存储进行机密性保护，防止其被非授权窃取。
6. 重要数据传输完整性：在密码基础设施区部署服务器密码机，并在应用服务器上部署国密安全密码应用中间件，采用SM2算法进行会话密钥交互，使用会话密钥采用HMAC-SM3算法在数据传输前对数据进行完整性保护，防止其被非授权篡改。
7. 重要数据存储完整性：在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用HMAC算法对数据信息存储进行完整性保护，防止其被非授权篡改。
8. 不可否认性：应使用安全电子签章系统对系统中重要数据进行数字签名，并对医疗处方信息进行电子签章，实现数据收发行为的不可否认性。

表 5.4 应用与数据安全保护对象

|  |  |  |
| --- | --- | --- |
| 序号 | 安全层面 | 保护对象 |
| 1 | 应用和数据安全 | 设备1 |
| 2 | 应用和数据安全 | 设备2 |

## 5.6 密**钥管**理

描述系统中各密钥全生命周期涉及的密钥管理方案和使用的独立的密钥管理设备、设施（若有）。

1. 密钥管理（还没设计通配符）

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **序号** | **密钥名称** | **算法** | **用途** | **存储位置** |
| 1 | {用户密钥} | {SM4} | {对数据加密密钥进行加密} | 服务器密码机 |

1. 密钥生命周期（还没设计通配符）

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **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 | 用户CA公钥 | 不涉及，由CA生产 | 以证书形式存储 | 以证书形式离线分发 | 以证书形式离线导入和导出 | 以证书形式使用 | 不涉及、由CA备份和恢复 | 不涉及、 由CA归档 | 不涉及、 由CA销毁 |

**5.7 密码应用部署（贾红豆）**

密码应用部署拓扑图如所示：

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



图 5.8 密码应用部署拓扑图

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

## 5.8 密码软硬件产品清单（刘双平）

通过上述分析，最终版测试系统的实现所需的密码产品所包括硬件、软件以及相关的服务如表 5.11所示。

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **序号** | **产品名称** | **部署位置** | **使用的密码算法** | **数量** | **用途** |
| 1 | 服务器密码机 | 基础设施区 | SM1/2/3/4 | 2 | 功能描述 |
| 2 | 时间戳服务器 | 基础设施区 | SM1/2/3/4 | 2 | 功能描述 |
| 3 | 签名验签服务器 | 基础设施区 | SM1/2/3/4 | 2 | 功能描述 |

**5.9 安全与合规性分析**

最终版测试系统的安全与合规性分析如表 5.12所示。

表 5.12 安全与合规性分析

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 指标要求 | 密码技术应用点 | 采取措施 | 标准符合性  （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 | 采用安全门禁系统实现进入人员身份鉴别 | 符合 | 无 |
| 电子门禁记录数据完整性 | 部署服务器密码机，使用HMAC对电子门禁记录数据和视频记录数据进行完整性保护 |
| 视频监控记录数据完整性 |
| 密码服务 | 密码应用技术服务 |
| 密码产品 | 服务器密码机 |
| 网络和通信安全 | 身份鉴别 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现通信实体身份鉴别，保证通信实体身份的真实性 | 符合 | 无 |
| 通信数据完整性 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现通信数据的机密性和完整性保护 | 符合 | 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 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现网络边界访问控制信息的完整性保护 | 符合 | 无 |
| 安全接入认证 | 在本地机房部署IPSec VPN安全网关、SSL VPN安全网关实现安全接入 | 符合 | 无 |
| 密码服务 | 数字证书认证服务 | 符合 | 无 |
| 密码产品 | SSL VPN、IPSec VPN、智能密码钥匙 | 符合 | 无 |
| 设备和计算安全 | 身份鉴别 | 在本系统运维人员PC端，配发USBKey，在密码基础设施区部署签名验签服务器，用户登录应用时验证人员数字签名，实现对登录应用用户的安全身份鉴别，防止非授权人员登录 | 符合 | 无 |
| 远程管理通道安全 | 采用遵循密码相关国家标准和行业标准的VPN技术，使用密码产品SSL VPN安全网关搭建安全的远程管理通道 | 符合 | 无 |
| 系统资源访问控制信息完整性 | 在密码基础设施区部署通过商用密码产品认证的服务器密码机，调用服务器密码机实现对系统资源访问控制信息进行完整性保护 | 符合 | 无 |
| 重要信息资源安全标记完整性 | - | 不适用 | 本系统不涉及重要信息资源的敏感标记 |
| 日志记录完整性 | 在密码基础设施区部署服务器密码机，调用服务器密码机，使用HMAC对应用服务器、数据库服务器等设备日志记录进行完整性保护 | 符合 | 无 |
| 重要可执行程序完整性、重要可执行程序来源真实性 | 在密码基础设施区部署签名验签服务器，应用服务器中所有重要程序或文件在生成时通过调用签名验签服务器使用SM3数字签名技术和SM2加密算法进行完整性保护；使用或读取这些程序和文件时，通过签名验签服务器进行验签以确认其完整性 | 符合 | 无 |
| 密码服务 | 数字证书认证服务、密钥管理服务 | 符合 | 无 |
| 密码产品 | SSL VPN安全网关、USBKey、服务器密码机、签名验签服务器 | 符合 | 无 |
| 应用和数据安全 | 身份鉴别 | 在本系统应用用户人员PC 端采用USBKey登录，在基础设施区部署签名验签服务器，用户登录应用时验证人员数字签名，实现对登录应用用户的安全身份鉴别，防止非授权人员登录 | 符合 | 无 |
| 访问控制信息完整性 | 在密码基础设施区部署服务器密码机，使用HMAC对系统应用的访问控制信息进行完整性保护，防止访问控制信息被篡改 | 符合 | 无 |
| 重要信息资源安全标记完整性 | - | 不适用 | 本系统不涉及重要信息资源的敏感  标记 |
| 重要数据传输机密性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2及SM3算法进行会话密钥交互，采用SM4算法对传输的数据信息进行机密性保护，防止其被非授权窃取 | 符合 | 无 |
| 重要数据存储机密性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用SM4算法对数据信息存储进行机密性保护，防止其被非授权窃取 | 符合 | 无 |
| 重要数据传输完整性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，采用SM2算法进行会话密钥交互，采用HMAC算法对传输的数据信息进行完整性保护，防止其被非授权篡改 | 符合 | 无 |
| 重要数据存储完整性 | 在密码基础设施区分别部署服务器密码机和国密安全密码应用中间件，使用HMAC对数据信息存储进行完整性保护，防止其被非授权篡改 | 符合 | 无 |
| 不可否认性 | 在基础设施区部署时间戳服务器，在系统中重要数据进行数字签名，并加盖时间戳，实现操作行为的不可否认性 | 符合 | 无 |
| 密码服务 | 密码应用技术服务 | 符合 | 无 |
| 密码产品 | 服务器密码机、国密安全密码应用中间件、签名验签服务器、时间戳服务器、可信浏览器、USBKey | 符合 | 无 |